



# Security Research Advances in 2009

**Konstantin (Kosta) Beznosov**

Laboratory for Education and Research in Secure Systems Engineering

Department of Electrical and Computer Engineering  
University of British Columbia, Canada

# venues

- **NDSS** -- Network & Distributed System Security Symposium, 8 - 11 February 2009, San Diego, CA, USA. (about 20 papers)  
<http://www.isoc.org/isoc/conferences/ndss/09/>
- **Oakland** -- IEEE Symposium on Security and Privacy (S&P 2009), 17-22 May 2009, Berkeley/Oakland, CA, USA. (about 20 papers)  
<http://oakland09.cs.virginia.edu/>
- **SOUPS** -- Symposium on Usable Privacy and Security (SOUPS), 15-17 July 2009, Mountain View, CA, USA. (about 20 papers)  
<http://cups.cs.cmu.edu/soups/2009/>
- **USENIX Security** Symposium, 10-14 August 2009, Montreal, Canada  
<http://www.usenix.org/events/sec09/> (about 20 papers)
- **CCS** -- ACM Computer and Communications Security Conference, 9-13 November 2009, Chicago, IL, USA  
<http://www.sigsac.org/ccs/CCS2009/> (about 40 papers)
- **ACSAC** -- Annual Computer Security Applications Conference, 8–12 December 2008, Anaheim, CA, USA (about 40 papers)  
<http://acsac.org/2008/>

the big four

total:

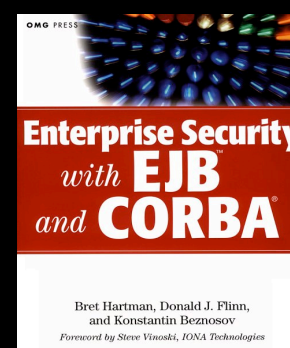
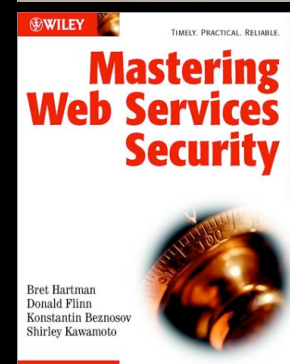
160-180 papers  
1,000 submissions

## selected papers

- Vanish: Increasing Data Privacy with Self-Destructing Data (USENIX Security)
- Measuring the security and reliability of authentication via 'secret' questions (Oakland)
- The Impact of Malicious Devices on a Cellular Network Core (CCS)
- Passport Cards, Enhanced Drivers Licenses, and other Security Applications of RFID tags (CCS)
- Tempest in a Teapot: Compromising Reflections Revisited (Oakland)
- Communicating Site Privacy Policies to Users (SOUPS)
- Improving Users' Mental Models of Personal Firewalls(SOUPS)

# Who's Konstantin (Kosta) Beznosov

- Education
  - M.S. (1997) & Ph.D. (2000) in CS, Florida International University
  - B.S. in Physics (1993), Novosibirsk State University, Russia
- Experience
  - Assistant Prof., Electr. and Comp. Egn., UBC (2003-present)
  - Directs Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
  - worked in US industry (1997-2003) as Security Architect:
    - end-user: Baptist Health Systems of South Florida
    - consulting: Concept Five Technologies,
    - software vendor: Hitachi Computer Products (America)
- Contributed to
  - Object Management Group (OMG)
    - CORBA Security revisions
    - Resource Access Decision (RAD)
    - Security Domain Membership Management (SDMM)
  - OASIS
    - eXtensible Access Control Markup Language (XACML) v1.0



# **Vanish: Increasing Data Privacy with Self-Destructing Data**

# The Problem: Two Huge Challenges for Privacy

## 1. Data lives forever

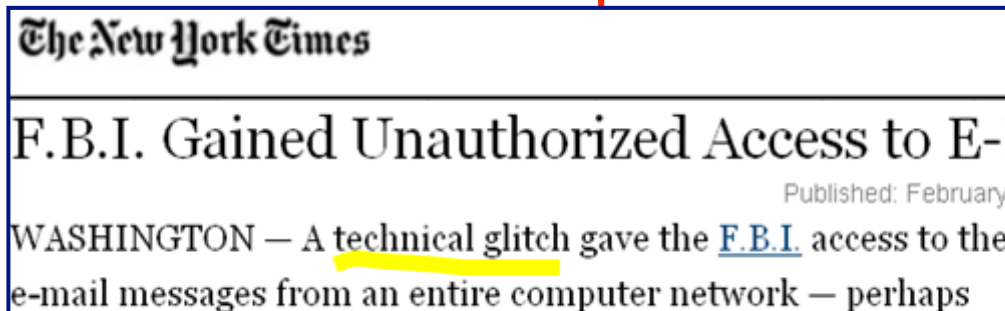
- On the web: emails,
- In the home: disks and
- In your pocket: phones



**The Washington Post**  
**Palin's Yahoo! Account Hacked**  
A group of computer hackers said yesterday they accessed a Yahoo! e-mail account of Alaska Gov. Sarah Palin, the Republican vice presidential nominee, publishing some of her private communications [...]

S, ...  
ata  
ge

## 2. Retroactive disclosure of both data and user keys has become commonplace



**The New York Times**  
**F.B.I. Gained Unauthorized Access to E-...**  
Published: February  
WASHINGTON — A technical glitch gave the F.B.I. access to the e-mail messages from an entire computer network — perhaps

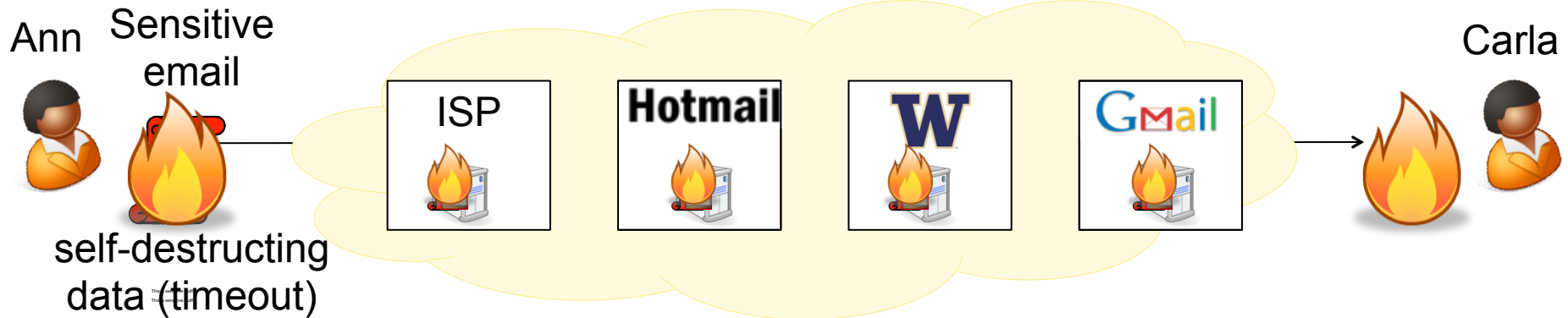


**WebProNews**  
Breaking eBusiness and Search News  
**Email Being Used More In Divorces**  
By Mike Sachoff - Mon, 02/11/2008 - 13:05  
The majority of U.S. divorce attorneys (88%) say there has been a significant increase in the number of cases using electronic evidence during the past five years, according to a survey by the American Academy of Matrimonial Lawyers (AAMLA).



**U.S. News & World Report**  
usnews.com  
**Seizing Laptops and Cameras Without Cause**  
A controversial customs practice creates a legal backlash

# Self-Destructing Data Model

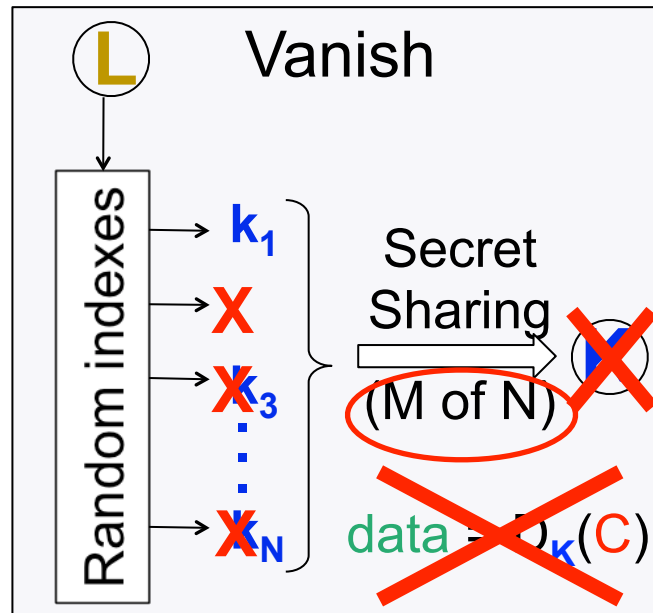
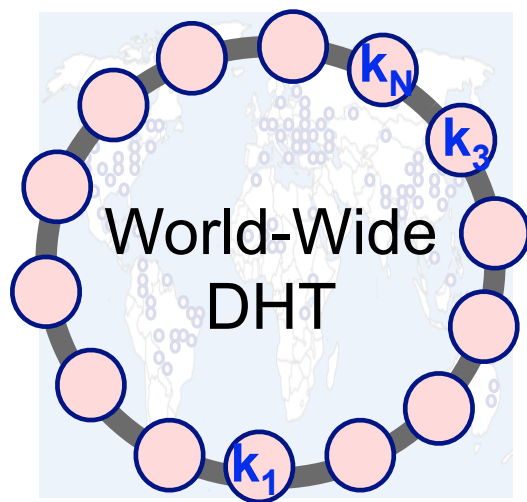


## Goals

1. Until timeout, users can read original message
2. After timeout, **all copies** become **permanently unreadable**
  - 2.1. even for attackers who obtain an **archived copy** & **user keys**
  - 2.2. without requiring **explicit delete action** by user/services
  - 2.3. without having to trust **any centralized services**

# How Vanish Works: Data Timeout

- The DHT **loses key pieces** over time
  - Natural churn: nodes crash or leave the DHT
  - Built-in timeout: DHT nodes purge data periodically



- **Key loss** makes all data copies **permanently unreadable**



## but don't hold your breath

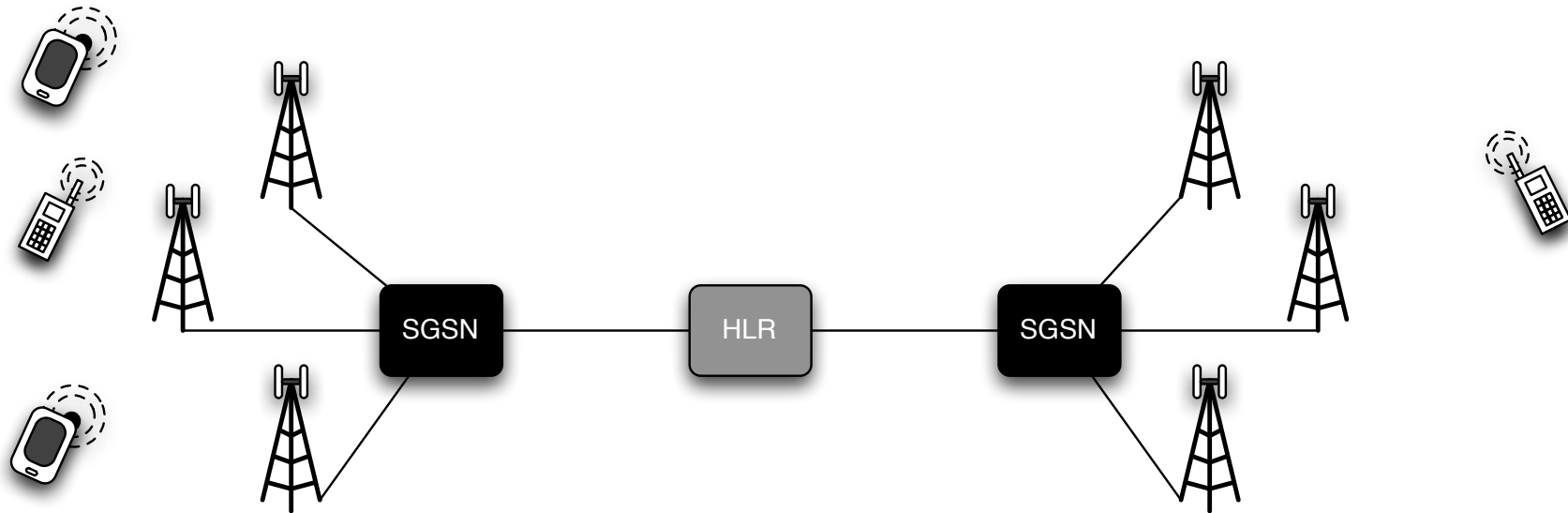
- S. Wolchuk, O. Hofmann, E. Felten, J. A. Halderman, C. Rossbach, B. Waters and E. Witchel, “Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs” to appear in NDSS '10



# On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core

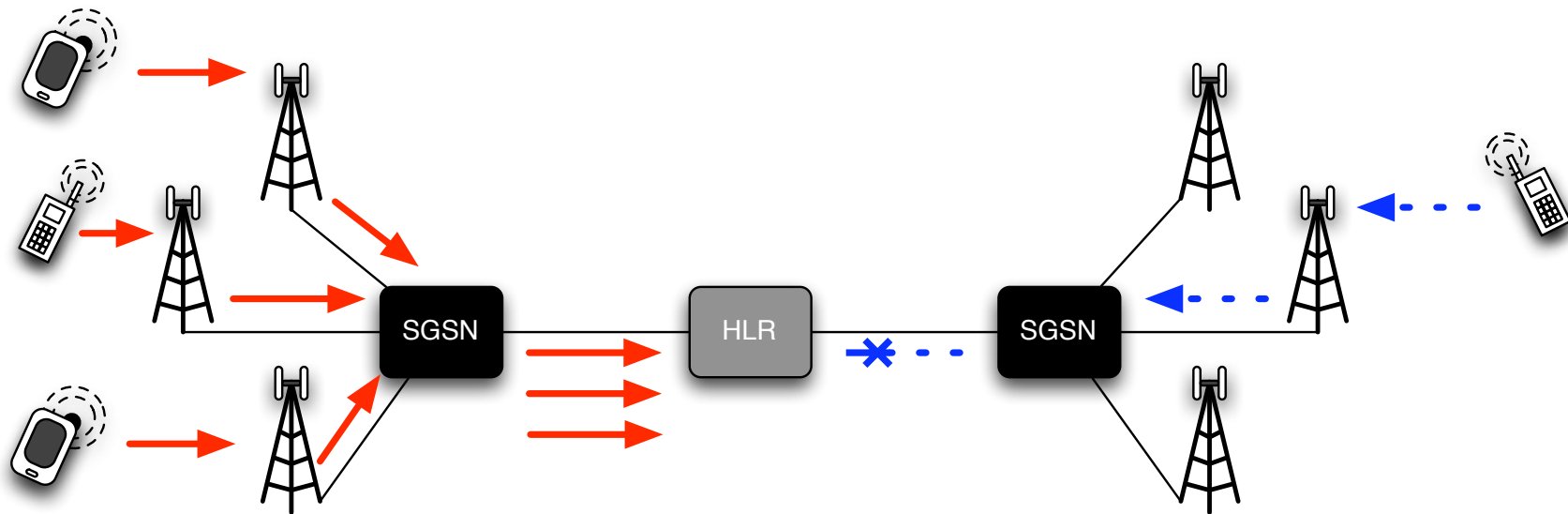
Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath  
Rao, Trent Jaeger, Patrick McDaniel and Thomas La Porta  
ACM CCS 2009

# Architecture



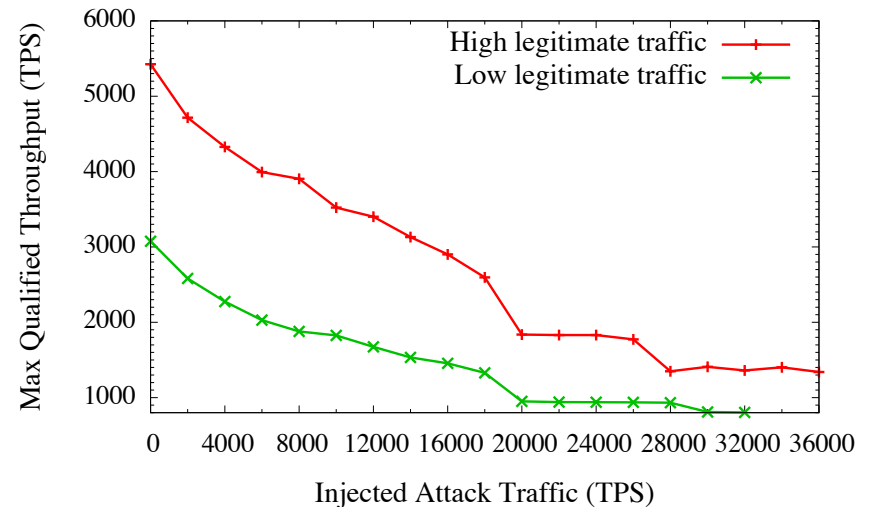
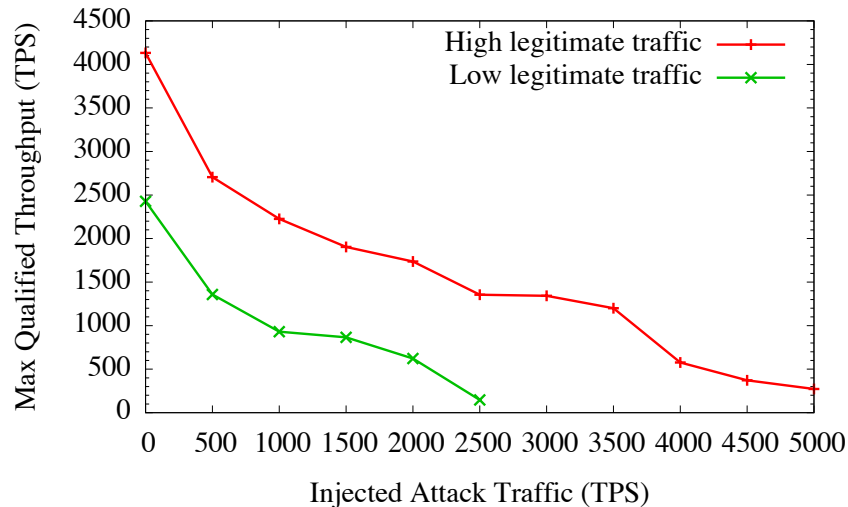
- Mobile Station (MS): User equipment and the target of infection
- Base Station (BS): The bridge between wired and wireless portions of the network.
- Serving GPRS Support Node (SGSN): Intelligent switch that can route voice and data traffic.
- Home Location Register (HLR): “DNS” of cellular networks, with critical differences...

# Architecture & Attack (High-Level)



- Serving GPRS Support Node (SGSN): Intelligent switch that can route voice and data traffic.
- Without an operational Home Location Register (HLR), not much can happen in a cellular network.
- Infected devices therefore send large amounts of traffic at the HLR in hopes of preventing legitimate requests.

# Device/Core Interactions



- In the class of currently deployed systems, 5000 attack messages per second drops throughput from 4132 TPS to 273 TPS.
  - ▶ 93% reduction in HLR throughput
- In more advanced systems, 30k attack messages per second drop throughput from 5424 TPS to 1340 TPS.
  - ▶ 75% reduction in HLR throughput

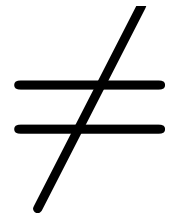
# How Big?

- For many current systems, an attacker would need to control 11,750 phones.
- For more capable HLRs, this number is closer to 141,000.



# Conclusion

- Increasing homogeneity and functionality of mobile phones makes them and their supporting infrastructure more susceptible to attack.
  - With a small number of malicious phones, area-code sized regions can be made largely (>90%) unreachable.
- Launching such attacks successfully is hard.
  - It requires that malware writers actually know something about the underlying network.
- Lesson: *These networks are different from the Internet. The same rules simply do not apply.*



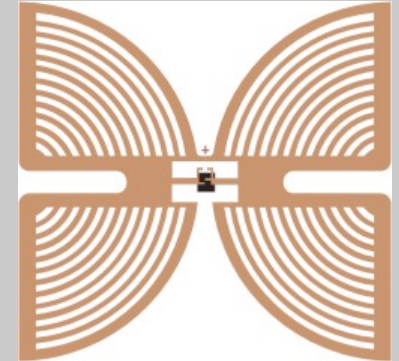
# Passport Cards, Enhanced Drivers Licenses, and other Security Applications of RFID Tags

Koscher, K., Juels, A., Brajkovic, V., and Kohno, T. "EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond," CCS '09, pp. 33-42. DOI= <http://doi.acm.org/10.1145/1653662.1653668>



# EPC Gen2 RFID Tags

- Electronic Product Code (EPC) essentially a “wireless barcode”
- Advantages over barcodes:
  - Can store more information (128 bits or more)
    - Enough to uniquely identify every object on Earth
  - Don't need line-of-sight
  - Larger read distances (up to 10 meters)
  - More durable

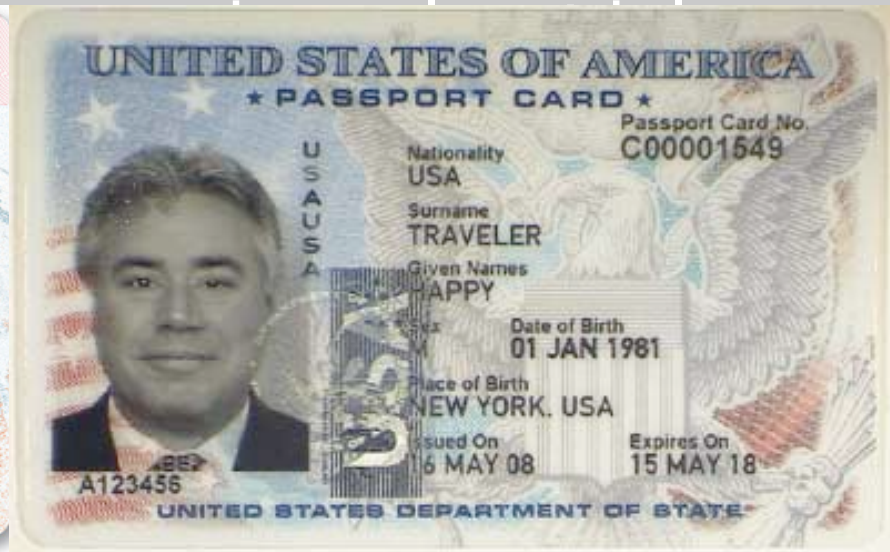


# Our Approach: A Case Study of WHTI

- Western Hemisphere Travel Initiative (WHTI)
- Phases-in strict ID requirements to travel between member countries
  - United States
  - Canada
  - Mexico
  - Bermuda
  - 17 nations in the Caribbean



# Case Study: WHTI



- WA Governor, BC Premier, US Government developed an alternative: The Enhanced Drivers License and Passport Card

# Case Study: WHTI

- Homeland Security mandated Gen2 tags in EDLs, Passport Cards
- We examine the security of these cards as a case study of using Gen2 in high-security applications



# Research Questions

- Vulnerability Analysis
  - What are the possible vulnerabilities?
  - What security mechanisms are deployed?
  - What are the read ranges?
- Countermeasures and Recommendations
  - Can we improve resistance to counterfeiting?
  - What are the “best practices?”

# Gen2 Security Features

- Two PINs:
  - KILL PIN – permanently disables tag



- ACCESS PIN – unlocks access-controlled operations (optional)

# Gen2 Security Features

- Optional write access control
  - Can be permalocked as well
- Optional read access control on PINs
  
- Tag ID (TID) memory bank can be factory set and locked and guaranteed to be unique
  - This is why many claim Gen2 to be “uncloneable”

# Read Range Experiments

- We only need a single read to clone a tag
- How far away can a tag be read?
- Depends on:
  - Tag / Reader
  - Reader Power
  - Environment
- We characterized EDL and Passport Card read ranges under a variety of environments



# Read Range Experiments

	Hallway		Outside	
	EDL	Passport	EDL	Passport
Held in hand	50m+	50m+	7.9m	7.2m
Empty backpack	50m+	50m+	10.5m	9.8m
Purse side pocket	50m+	50m+	8.3m	1.9m
Wallet; in purse	11.3m	2.8m	5.9m	0.5m
Wallet; in front pocket	8.9m	0.6m	2.4m	1.9m

# Beyond Cloning

- EPC IDs are just globally unique numbers
  - ... so are Social Security Numbers
- Can track where a person goes
- Can track how frequently a person visits a location
- Can remotely identify US citizens abroad

# paper summary

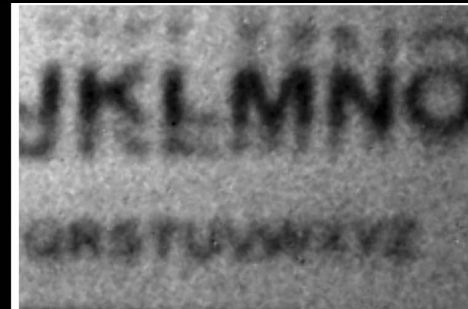
- We explored challenges in deploying EPC Gen2 RFID tags in security applications
- We use the Washington Enhanced Drivers License and Passport Card as a case study
- We characterized read ranges with respect to privacy
- We showed that anti-cloning techniques proposed by Juels are practical
- We developed a set of recommendations to improve WHTI card security



# Reading Computer Screen from Eye Reflection

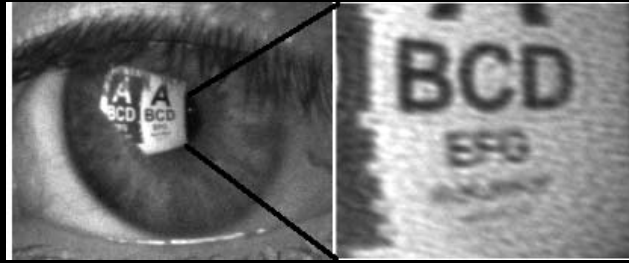
M. Backes, T. Chen, M. Duermuth, H. P.A. Lensch, M. Welk,  
"Tempest in a Teapot: Compromising Reflections Revisited," Oakland '09, pp. 315-327,  
DOI: <http://doi.ieeecomputersociety.org/10.1109/SP.2009.20>.

# previous results: reflections in a tea pot



Reflections in a tea pot, taken from a distance of 10m.  
The 18pt font is readable from the reflection.

# new results: reflections in the eye









Reflections captured in the eye from a distance of 10 meters.

- 36pt font from a distance of 10 meters
- previously 150pt font from 4 meters.

# Improving Users' Mental Models of Personal Firewalls

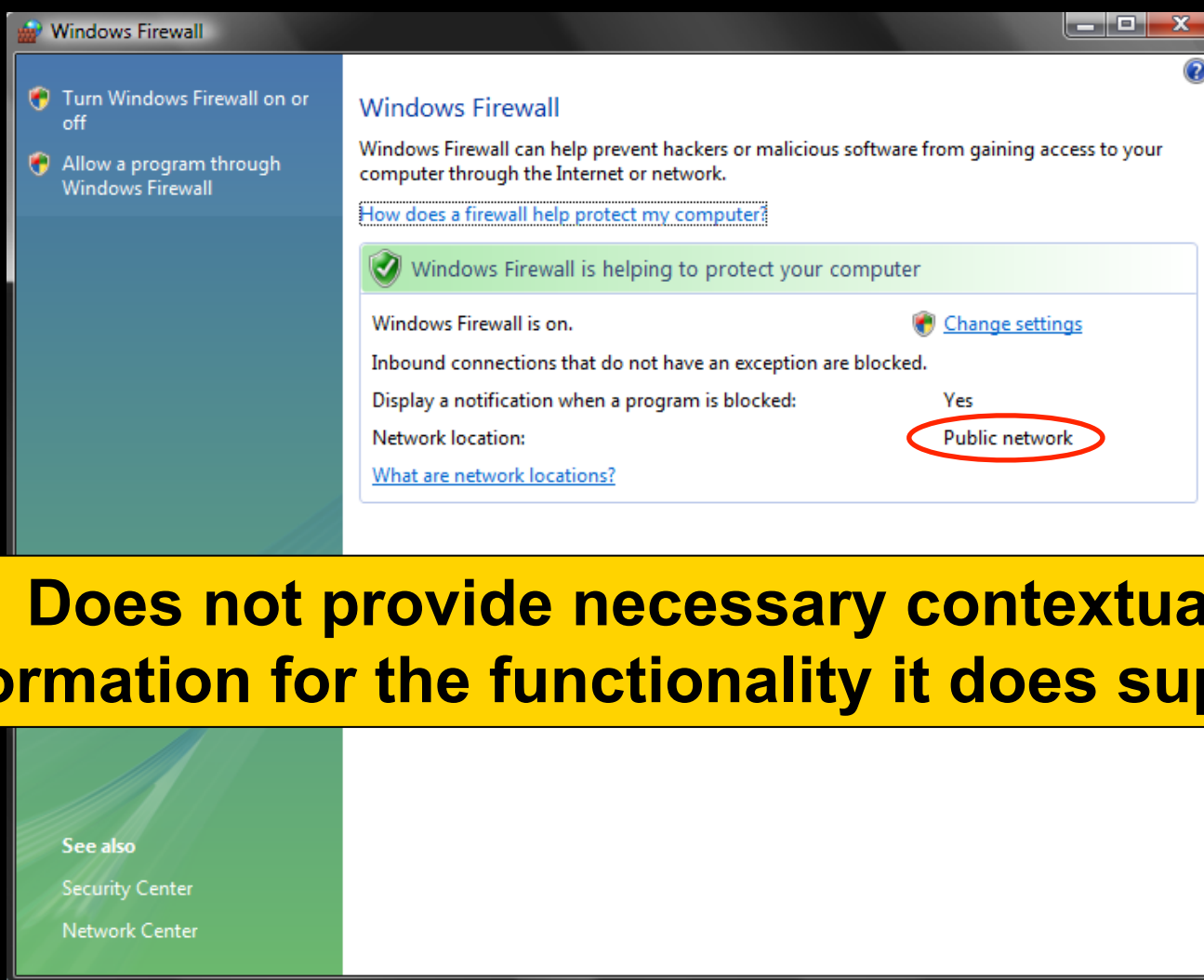
F. Raja, K. Hawkey, and K. Beznosov,  
“Revealing hidden context: improving mental models of personal firewall users,”  
SOUPS '09, pp. 1-12, DOI= <http://doi.acm.org/10.1145/1572532.1572534>

# Network Context in Vista Firewall

	Public Network Location 	Private Network Location 	Domain Network Location 
Wireless Network Connection 	On	Off	On
Local Area Connection 	On	Off	On
Bluetooth Network Connection 	Off	Off	Off



# Limited functionality and simplified interface to hide complexity from user



**Does not provide necessary contextual information for the functionality it does support**

Changes applied **only** to profile associated with current network location and that is not obvious

The image shows two overlapping windows from Windows Firewall. The background window, titled 'Windows Firewall', displays a status message: 'Your computer is not protected. Windows Firewall is off.' This message is circled in red. Below it, it says 'Network location:' followed by a link 'What are network locations?'. A yellow warning box below that states 'Windows Firewall is not using settings to protect your computer. See recommended settings?'. At the bottom, there are links for 'See also', 'Security Center', and 'Network Center'. The foreground window, titled 'Windows Firewall Settings', has the 'General' tab selected. It shows a green checkmark icon and the text 'Windows Firewall is helping to protect your computer'. Below this, it explains that Windows Firewall can help prevent hackers or malicious software from gaining access. There are three radio button options: 'On (recommended)' (which is selected), 'Block all incoming connections', and 'Off (not recommended)'. Each option has a brief description. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons, and a link 'Tell me more about these settings'.

Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

### Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

[How does a firewall help protect my computer?](#)

Windows Firewall is not using the recommended settings.

Windows Firewall is on.

[Change settings](#)

Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

Network location: Public network

[What are network locations?](#)

Windows Firewall is not using the recommended settings to protect your computer. [What are the recommended settings?](#) [Update settings now](#)

Security Center

Network Center

**Simplified interface:**

- Hidden network context
- Automatic switching of firewall profiles

# alternative interface

The screenshot shows the Windows Firewall control panel window. On the left, there are three main options: "Turn Windows Firewall on or off", "Allow a program through Windows Firewall", and "See also" with links to "Security Center" and "Network Center". The main content area is titled "Windows Firewall" and includes a description: "Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network." Below this, it asks "How does a firewall help protect my computer?" and lists three network locations: "Public Network" (with a bench icon), "Private Network" (with a house icon), and "Domain Network" (with a computer icon). Each location has a "Change settings for" link. A large diagram overlay shows a globe on the left and a computer on the right, with a brick wall representing the firewall. Red arrows represent "Local Area Connection", a green arrow represents "Wireless Network Connection", and a blue arrow represents "Bluetooth Network Connection". A yellow starburst is shown where a connection is blocked by the wall. Below the diagram is a table of connection settings:

Connection	Firewall Status	On	Off
Bluetooth Connection	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>

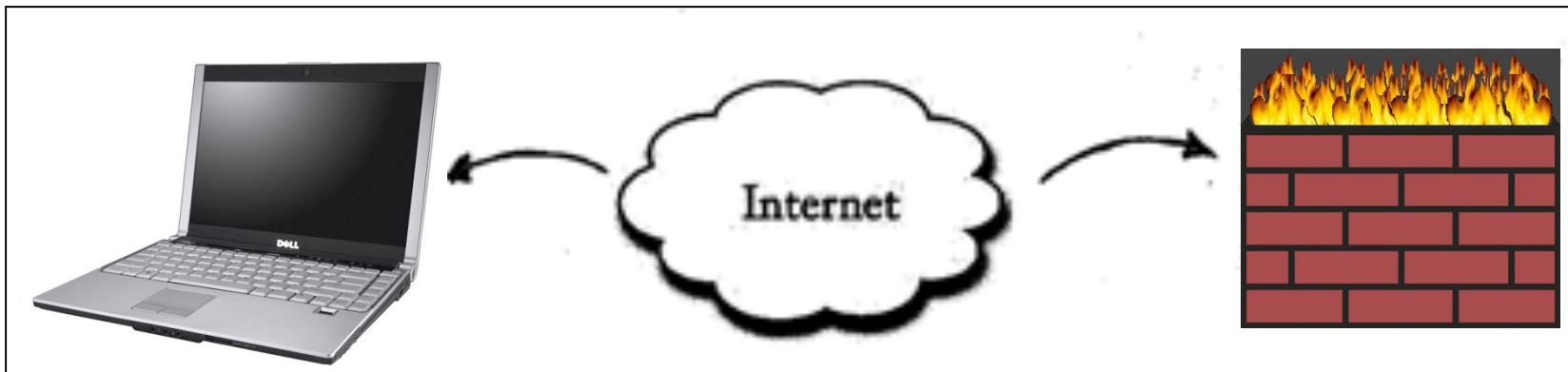
Below the table, there are two main options with checkboxes and radio buttons:

- [Turn Windows Firewall On for All Network Locations and Connections \(recommended\)](#)  
This setting blocks outside sources from connecting to this computer, except for those unblocked on the Exceptions tab above.
- [Turn Windows Firewall Off for All Network Locations and Connections \(not recommended\)](#)  
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

At the bottom, there is a link "Tell me more about these settings" and "OK" and "Cancel" buttons.

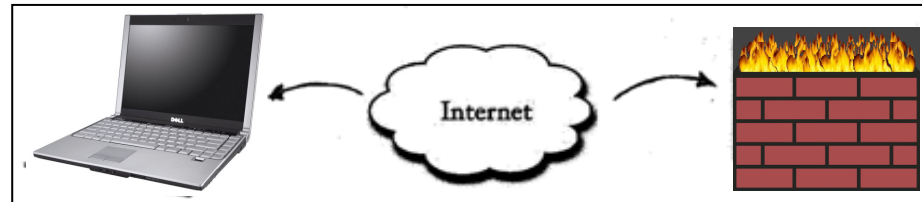
# Mental Models

- **Incorrect:** incorrect basic understanding of firewall operation

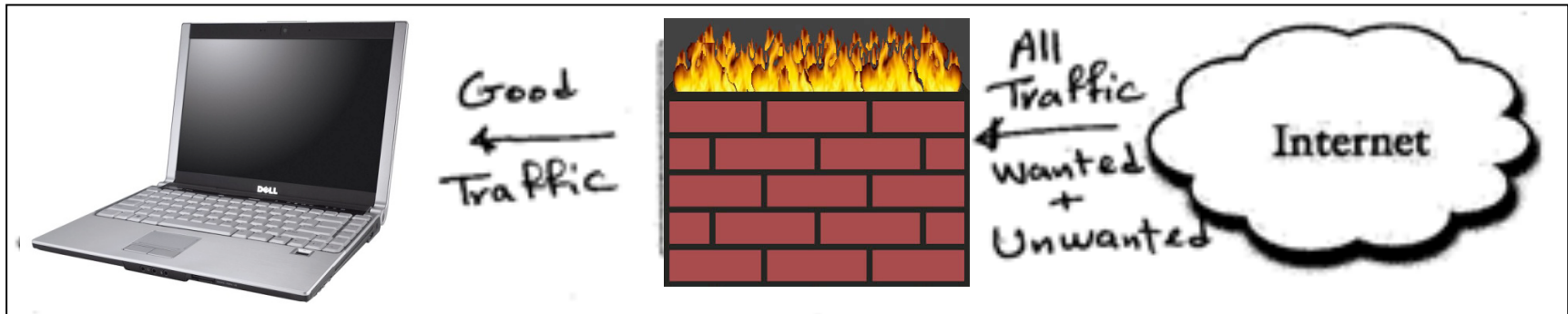


# Mental Models

- Incorrect

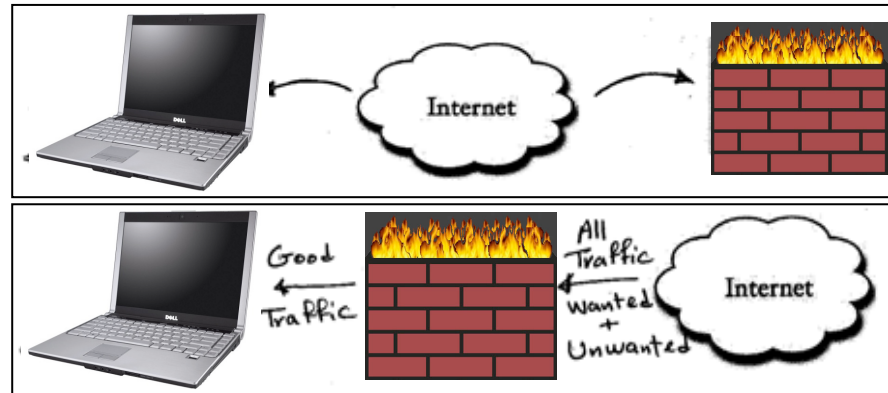


- **Incomplete:** correct basic understanding of firewall operation, without context of network location and connection

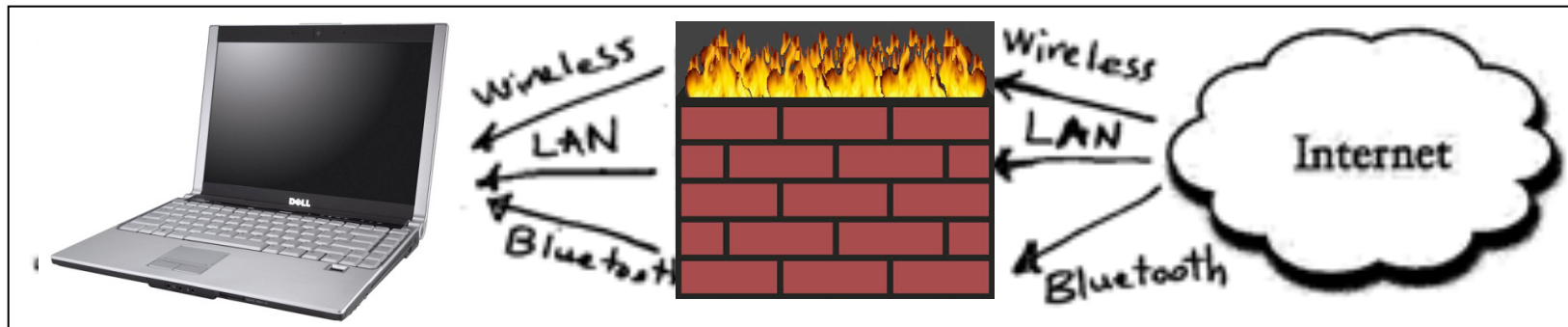


# Mental Models

- Incorrect
- Incomplete



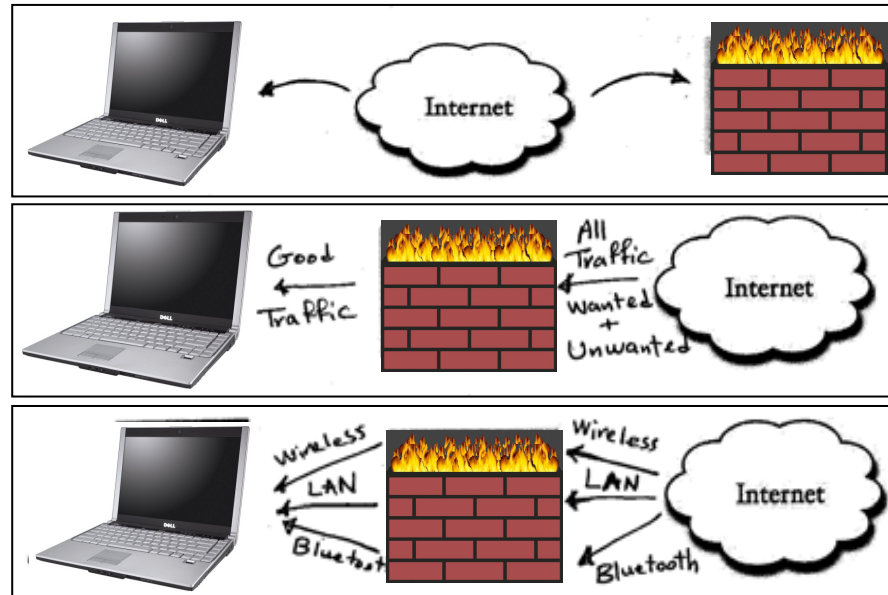
- **Partially complete:** correct basic understanding of firewall operation, with either context of network location or connection



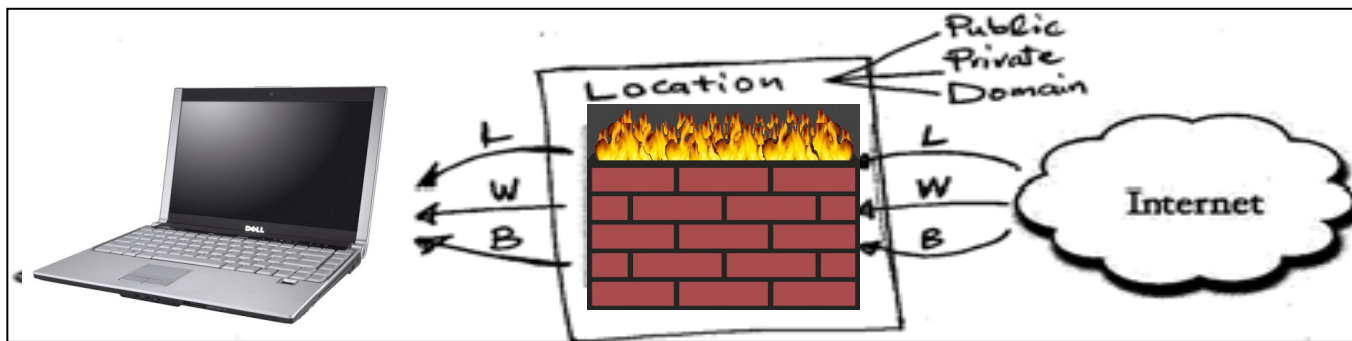
39

# Mental Models

- Incorrect
- Incomplete
- Partially complete

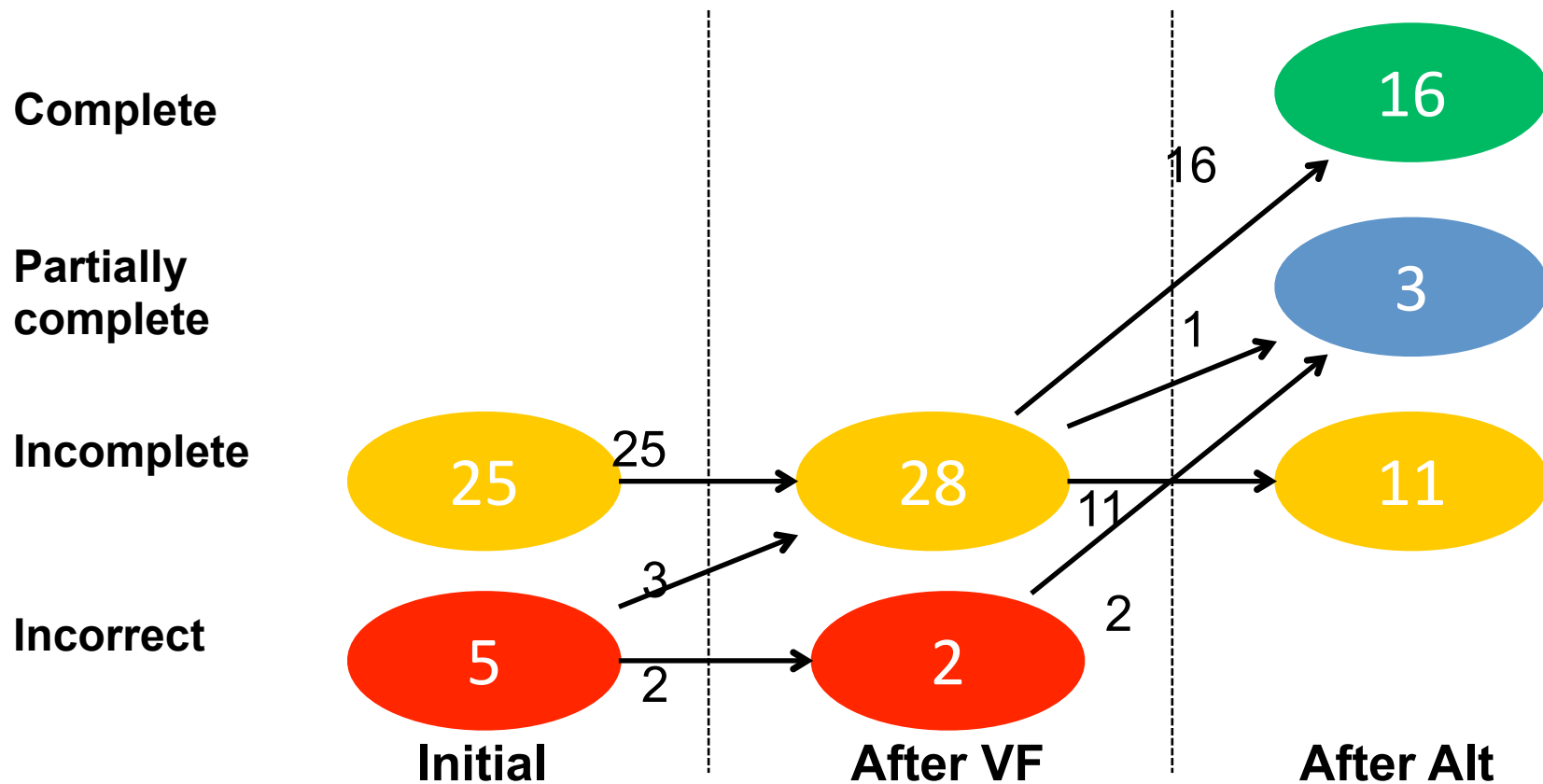


- **Complete:** correct basic understanding of firewall operation, with both context of network location and connection

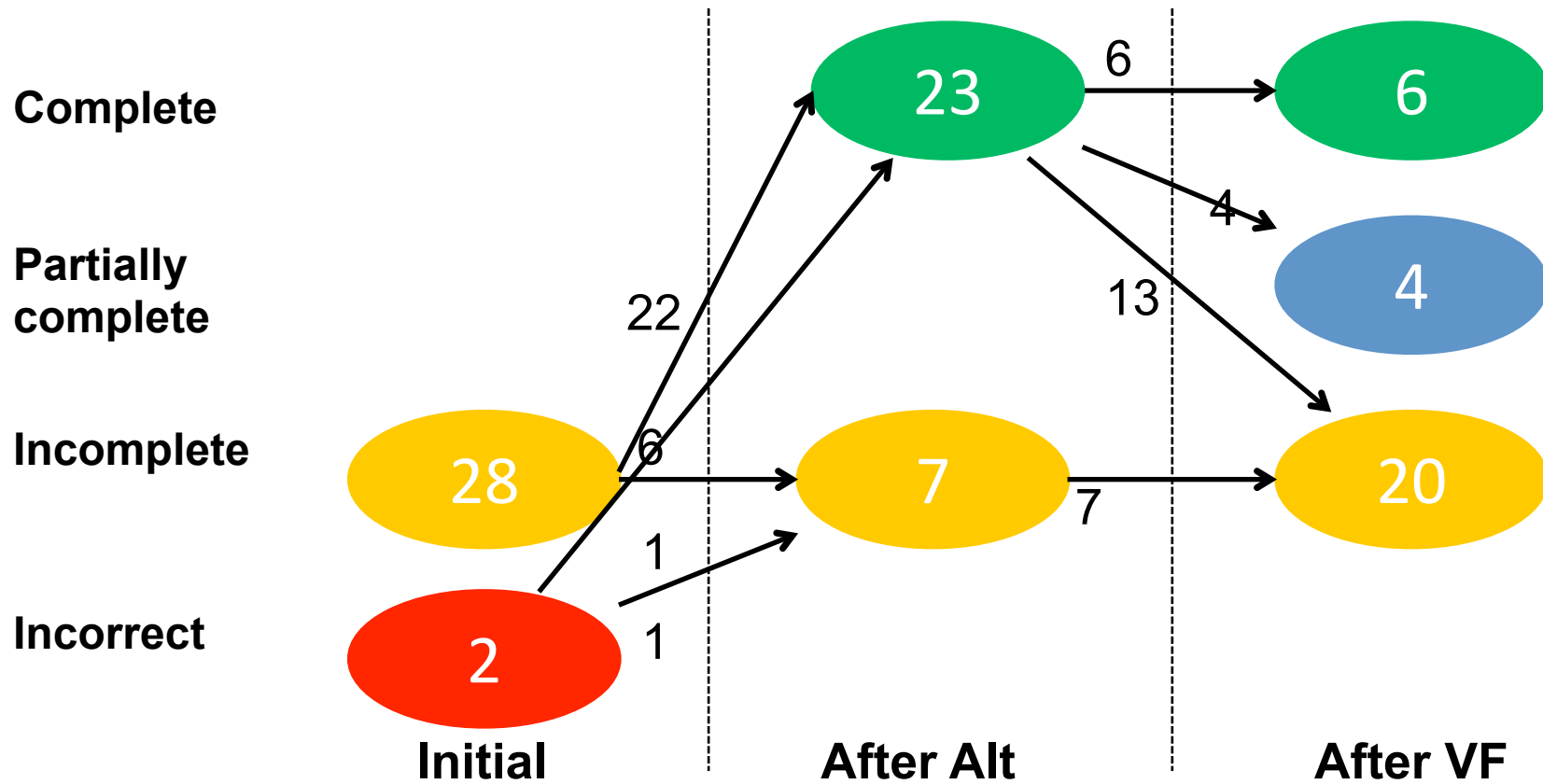




# First Vista Firewall Basic, then Alternative



# First Alternative, then Vista Firewall Basic



# **It's No Secret!**

## **Measuring the security and reliability of authentication via 'secret' questions**

S. Schechter, B. Brush, S. Egelman, "It's No Secret. Measuring the Security and Reliability of Authentication via," Oakland '09, pp.375-390  
DOI: <http://doi.ieeecomputersociety.org/10.1109/SP.2009.11>



Republican vice presidential candidate, Alaska Gov., Sarah Palin, answers a supporter's question during a town hall style meeting in Grand Rapids, Mich., Wednesday night, Sept. 17, 2008.

## Hacker impersonated Palin, stole e-mail password

By TED BRIDIS – Sep 18, 2008

WASHINGTON (AP) — Details emerged Thursday behind the break-in of Republican vice presidential candidate Sarah Palin's e-mail account, including a first-hand account suggesting was vulnerable because a hacker was able to impersonate her online to obtain her password.

The hacker guessed that Alaska's governor had met her husband in high school, and knew Palin's date of birth and home Zip code. Using those details, the hacker tricked Yahoo Inc.'s service into assigning a new password, "popcorn," for Palin's e-mail account, according to a chronology of the crime published on the Web site where the hacking was first revealed.

# Methodology:

## First session

- **Invited pairs of acquaintances to participate**
  - Friends, family members, coworkers, etc.
- **Asked participants to answer all questions**
  - Report if unable to answer or uncomfortable doing so
  - Minimum 2 characters per answer
  - Incentive for future recall
    - Increased chance to win an Xbox 360
  - Did not yet disclose they would be guessing their partner's answers (or vice versa)

# Methodology:

## First session (cont.)

- **Asked participants how much they trusted their partners**
  - “Would you trust your partner with your hotmail password?”
- **Asked participants to guess their partners' answers**
  - Correct guesses increased chance to win Xbox 360
  - Worth five times more than correct recall
- **Asked to recall answers at end of study session**
  - Kept promise to increase chance of winning the Xbox 360
  - Gave participants impression memory study complete

# Methodology:

## Longitudinal follow-up

- Emailed participants 3-6 months later
- Asked to recall their answers
  - Online tool reported if they recalled correctly
  - Unlimited number of guesses allowed
- Base gratuity + performance-based gratuity
  - \$15, \$10, \$5, or \$0 based on performance quartile

# Are there any good questions?

Forgot	Statistically guessable	Guessed by untrusted partner	Question
14%	10%	17%	Mother's maiden name?
5%	5%	2%	What was your father's middle name?
17%	—	—	What was your first phone number?
9%	1%	—	What was the name of your first school?
21%	8%	13%	When was your first job?
18%	1%	11%	Best childhood friend
21%	—	4%	Favorite teacher
25%	6%	7%	What is your favorite restaurant?
15%	1%	8%	Who is your favorite singer?
23%	6%	—	What was your first teacher's name?

**NO!**



# Short-term solutions

- Discourage use of popular answers
- Reduce number of guesses allowed if guesses are among popular answers
  - Mother's birthplace:  
Los Angeles; New York; Mumbai; Shanghai
- Increase number of guesses allowed if guesses are similar to each other
  - Mother's birthplace:  
Berkeley, CA; Berkeley; Oakland; San Francisco

# findings summary

- Rarely are answers to 'secret' questions both
  - sufficiently secret *and*
  - sufficiently memorable
- User-written questions are no better
- Better backup authentication options needed

# Other backup authentication options?

- **Employ your social network**
  - Identify *trustees* – people you trust – in advance
  - Let trustees verify your identity when all else fails
  - Set authentication threshold –  $k$  of  $n$  trustees – to trade off reliability for security
- **Prior work**
  - *Fourth-factor authentication: Somebody you know*  
Brainard *et al.*, ACM CCS 2006

# Communicating Site Privacy Policies to Users

P. Kelley, J. Bresee, L. Cranor, R. Reeder, "A "nutrition label" for privacy"  
SOUPS '09, DOI= <http://doi.acm.org/10.1145/1572532.1572538>

# privacy statement examples

Click Here to Install Silverlight Canada Change | All Microsoft Sites

**Microsoft** Search Microsoft.com for:

## Microsoft Online Privacy Notice Highlights

(last updated May 2008)



### Scope

This notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft Web sites and services that display or link to this notice.

### Personal Information

#### Additional Details

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

### Your Choices

#### Additional Details

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you by e-mail, telephone, and postal mail, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
- To opt-out of the display of personalized advertisements, go to the [Display of Advertising](#) section of the full privacy statement.
- To view and edit your personal information, go to the [access section](#) of the full privacy statement.

### Uses of Information

#### Additional Details

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

### Important Information

- The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Windows Live ID](#).
- For more information on how to help protect your personal computer, your personal information and your family online, visit our [online safety resources](#).
- Microsoft is a member of the [TRUSTe](#) privacy seal program.

### How to Contact Us

For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using our [Web form](#). If you have a technical or general support question, please visit <http://support.microsoft.com> to learn more about Microsoft Support offerings.

## Apple Customer Privacy Policy

Apple's Customer Privacy Policy covers the collection, use, and disclosure of personal information that may be collected by Apple anytime you interact with Apple, such as when you visit our website, when you purchase Apple products and services, or when you call our sales or support associates. Please take a moment to read the following to learn more about our information practices, including what type of information is gathered, how the information is used and for what purposes, to whom we disclose the information, and how we safeguard your personal information. Your privacy is a priority at Apple, and we go to great lengths to protect it.

### Why we collect personal information

We collect your personal information because it helps us deliver a superior level of customer service. It enables us to give you convenient access to our products and services and focus on categories of greatest interest to you. In addition, your personal information helps us keep you posted on the latest product announcements, software updates, special offers, and events that you might like to hear about.

If you do not want Apple to keep you up to date with Apple news, software updates and the latest information on products and services click [www.apple.ca/contact/myinfo](http://www.apple.ca/contact/myinfo) and update your personal contact information and preferences.

### What information we collect and how we may use it

There are a number of situations in which your personal information may help us give you better products. For example:

- We may ask for your personal information when you're discussing a service issue on the phone with an associate, downloading a software update, registering for a seminar, participating in an online survey, registering your products, or purchasing a product.
- When you interact with Apple, we may collect personal information relevant to the situation, such as your name, mailing address, phone number, email address, and contact preferences; your credit card information and information about the Apple products you own, such as their serial numbers and date of purchase; and information relating to a support or service issue.
- We also collect information for market research purposes — such as your occupation and where you use your computer — to gain a better understanding of our customers and thus provide more valuable service.
- We collect information regarding customer activities on our websites, .Mac, and the iTunes Store. This helps us to determine how best to provide useful information to customers and to understand which parts of our websites, products, and Internet services are of most interest to them.
- We may use personal information to provide products that you have requested as well as for auditing, research, and analysis to improve Apple's products.

### Your Apple ID and related information

The Apple website, as well as Apple services such as .Mac and the iTunes Store, allows you to create an "Apple ID" based on your personal information. This convenient service saves you time and allows for easier use of our web services. Here's how it works: You create a personal profile — providing your name, phone number, email address, and in some cases your mailing address or a credit card number — and choose a password and password hint (such as the month and day of your birth) for security. The system saves your information and assigns you a personal Apple ID — in many cases simply your email address, because it's unique and easy to remember. The next time you order from the Apple Store or register a new product, all you need to do is enter your Apple ID and password; the system looks up the information it needs to assist you. In addition, if you update the information associated with your Apple ID it will be available for all your transactions with Apple globally.

### iCards and gift services

Apple also enables you to send "iCards", set up allowances on the iTunes Store and purchase and send gift certificates and products, to family members, friends or colleagues. To fulfill your request, Apple may require personal information about the person to whom you are sending the product or service such as their name, physical address, email address, and so on. The personal information you provide about that person is used only for the purpose for which it is collected. Apple will not use the information collected to market directly to that person.

### Publicly displayed information is public

If you use a bulletin board or chat room on an Apple website you should be aware that any information you share is visible to other users. Personally identifiable information you submit to one of these forums can be read, collected, or used by other individuals to send you unsolicited messages. Apple is not responsible for the personally identifiable information you choose to submit in these forums. For

Apple is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, nonprofit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. Because Apple wants to demonstrate our commitment to your privacy, we have agreed to disclose our information privacy practices for compliance review by TRUSTe.



The TRUSTe trademark reflects our promise to tell you what personal information we collect; the types of companies we may share your information with; the choices available to you regarding the collection, use, and distribution of the information; the security procedures in place to protect the loss or misuse of information under our control; and how you can correct inaccuracies in the information. The TRUSTe program covers only information that is collected through this Web site, and does not cover information that may be collected through software downloaded from the site.

If you have questions or concerns about Apple's collection, use, or disclosure of your personal information, please email us at [privacy@apple.com](mailto:privacy@apple.com). If Apple doesn't respond or your inquiry hasn't been addressed to your satisfaction, please visit the TRUSTe website for contact information. This certification applies to all sites under the apple.com domain.

# A "nutrition label" for privacy

## The Acme Policy

types of information this site collects	how we use your information			who we share your information with	
	marketing	telemarketing	profiling	other companies	public forums
contact information	opt out	opt out		opt in	
cookies	opt out	opt out		opt in	
preferences	opt out	opt out		opt in	!
purchasing information	opt out	opt out		opt in	
social security number & gov't ID					
your activity on this site	opt out	opt out		opt in	!

**Information not collected or used by this site:** demographic, financial, health, location.

### Access to your information

This site gives you access to your contact data and some of its other data identified with you

acme.com  
5000 Forbes Avenue  
Pittsburgh, PA 15213 United States  
Phone: 800-555-5555  
help@acme.com

### How to resolve privacy-related disputes with this site

Please email our customer service department



we **will** collect and use your information in this way



by default, we **will** collect and use your information in this way unless you tell us not to by opting out



we **will not** collect and use your information in this way



by default, we **will not** collect and use your information in this way unless you allow us to by opting in

# papers summary

- Vanish: Increasing Data Privacy with Self-Destructing Data (USENIX Security)
- Measuring the security and reliability of authentication via 'secret' questions (Oakland)
- The Impact of Malicious Devices on a Cellular Network Core (CCS)
- Passport Cards, Enhanced Drivers Licenses, and other Security Applications of RFID tags (CCS)
- Tempest in a Teapot: Compromising Reflections Revisited (Oakland)
- Communicating Site Privacy Policies to Users (SOUPS)
- Improving Users' Mental Models of Personal Firewalls(SOUPS)



Konstantin (Kosta) Beznosov  
Ph.D., P.Eng.

[konstantin.beznosov.net](http://konstantin.beznosov.net)

Laboratory for  
Education and Research in  
Secure Systems Engineering  
[lersse.ece.ubc.ca](http://lersse.ece.ubc.ca)

The logo features a collage of images in the background, including a person in a lab coat working with equipment, a person at a computer workstation, and a control room with multiple monitors. The text is overlaid on this collage in a serif font, with the words 'Education', 'Research', 'Secure', and 'Engineering' in red, and 'Laboratory for', 'and', 'in', 'Systems', and 'ersse.ece.ubc.ca' in black.