Security: Computing in an Adversarial Environment

Presenter
Dr. Carrie Gates
CA Technologies
carrie.gates@ca.com

Moderator
Dr. Christopher W. Clifton
Purdue University
clifton@cs.purdue.edu

Association for Computing Machinery
Advancing Computing as a Science & Profession

ACM Learning Center
(http://learning.acm.org)

- 1,300+ trusted technical books and videos by leading publishers including O'Reilly

- Online courses with virtual labs and assessment exams

- ACM Tech Packs on big current computing topics: Annotated Bibliographies compiled by subject experts

- ACM Learning Paths providing unique, accessible entry points into popular languages such as Python and Ruby

Introductions

- Carrie Gates, *CA Labs*

- Christopher Clifton, *Purdue University*

What makes security different from every other computer science discipline?

Random (Camera) Questions

1. Think back to the last time you went into a bank. How many cameras were there?
2. Where have you started seeing cameras, besides the obvious places like banks?
3. What happens if you happen to put your coat over the camera on a flight check-in kiosk when checking in for an international flight?
4. Where can you stand while getting cash out of a bank machine so that the camera doesn't get a picture of you?

Association for Computing Machinery
Advancing Computing as a Science & Profession

Random (Other) Questions

5. What ID is needed to pick up your car from being serviced? Or even just your dry cleaning?
6. What do you need to pick up a FedEx parcel held at the front office of your apartment complex?
7. Can you get through TSA without an ID?
8. How close can you get to the US president at an APEC 2007 summit by pretending to be Canada?
    - http://www.youtube.com/watch?v=SypnEO9wMtI (1:45 in)
9. Can I make someone with a pacemaker have a heart attack?

Random (Other) Questions

10. Can I read someone’s computer screen just from a reflection?
    - *Tempest in a Teapot: Compromising Reflections Revisited* by M. Backes (2009)
11. Can I get into grad school without the prereqs?

What do all those questions have in common?

Security Mindset

- A way of looking at the world that makes you discover the holes first.

- “*… the security mindset involves thinking about how things can be made to fail.*” – Bruce Schneier

Security Primitives

CIA

Security Services:

- Confidentiality
  - Keep my secrets secret!
- Integrity
  - The data is what it is supposed to be
- Availability
  - From anywhere at anytime

Computer Security: Art and Science by Matt Bishop (2003)
http://www.informit.com/articles/article.aspx?p=30710

Association for Computing Machinery

Advancing Computing as a Science & Profession

Why?

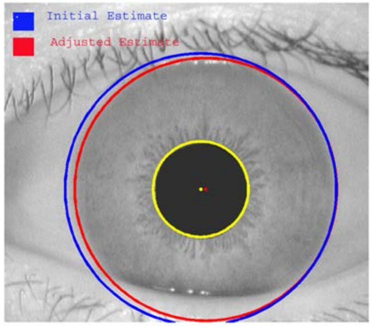
What are the goals of security?

- Protection (of people, of assets)
- Assurance
- Trust
- Legal Compliance
- Governance

AAA

How do we protect systems?

- Authentication
  - Passwords, biometrics, tokens
- Authorization
  - Access control
- Audit (Accounting)
  - Intrusion detection, forensic analysis



Ultimate Goal: Accountability

- Risk Analysis × Threats = Policy

“Thing is that once the security mindset matures with experience we *know* that it is possible for any system, regardless of physical location or vendors that supply software, to be compromised. The question the risk analyst must answer however, is really ‘What is *probable*?’.” – Alex @ http://riskmanagementinsight.com/riskanalysis/?p=350

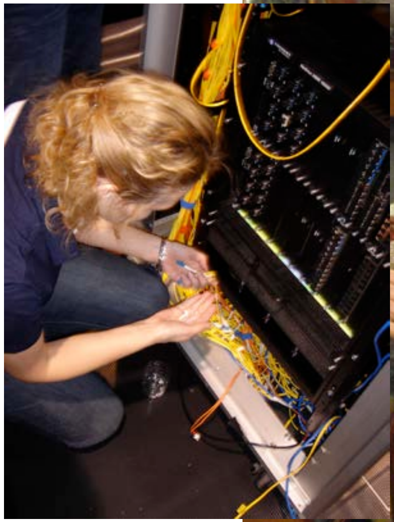
Security and Society

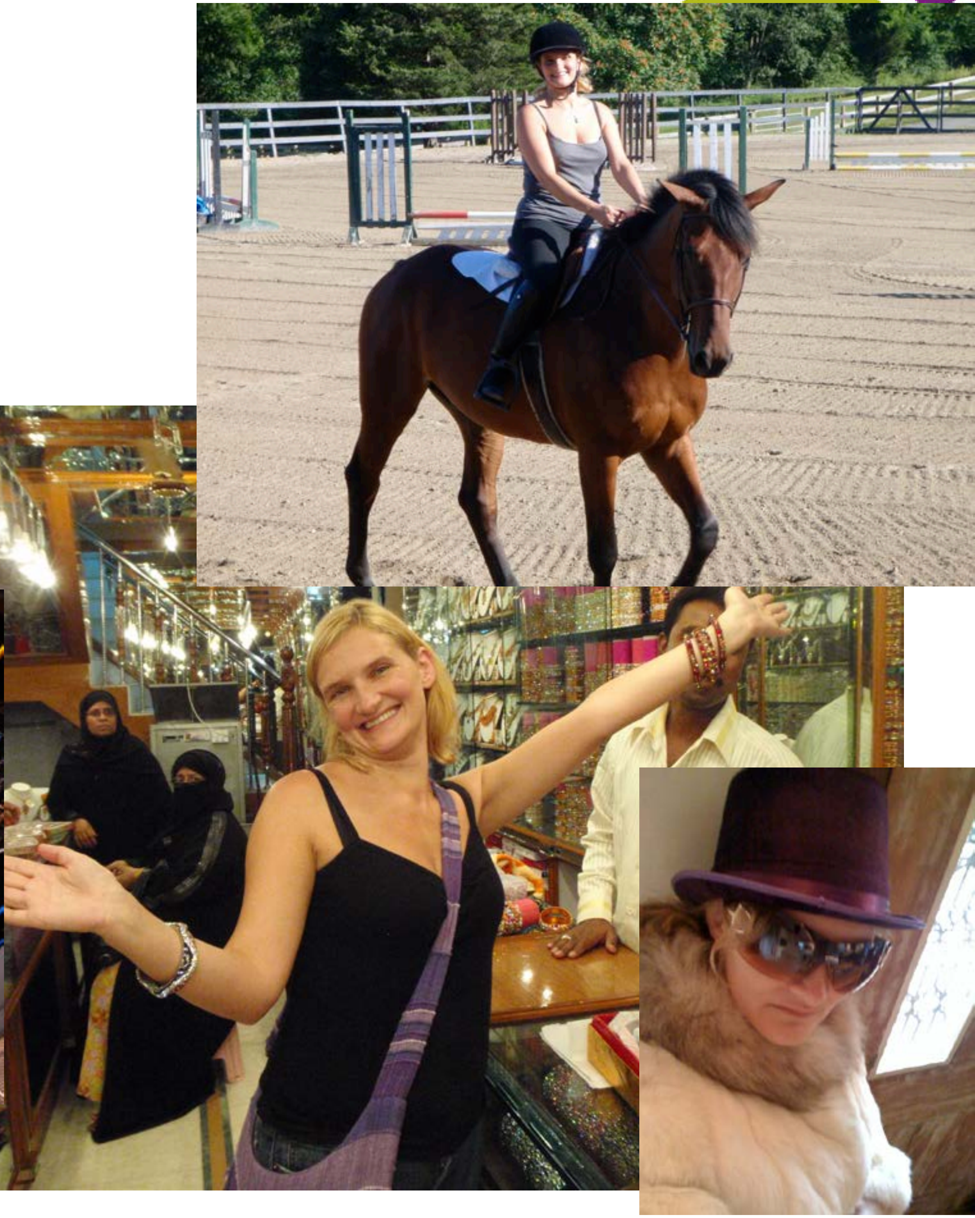
Identity

- What is your identity?

Who am I? ☺

- PII: Name / Address / SSN
- Genetics
- Position at work
- Hobbies





Association for
Computing Machinery

Advancing Computing as a Science & Profession

Identity

- What is your identity?
- How do you know you are giving access to the right person?
  - Root of the authentication problem
  - Continuous authentication
- Should there be a global identity? (E.g., NSTIC)
  - Or should your identities be kept separate?
- What about anonymity? Or pseudonymity?
  - Attribution problem

Identity Woman:
http://www.identitywoman.net/

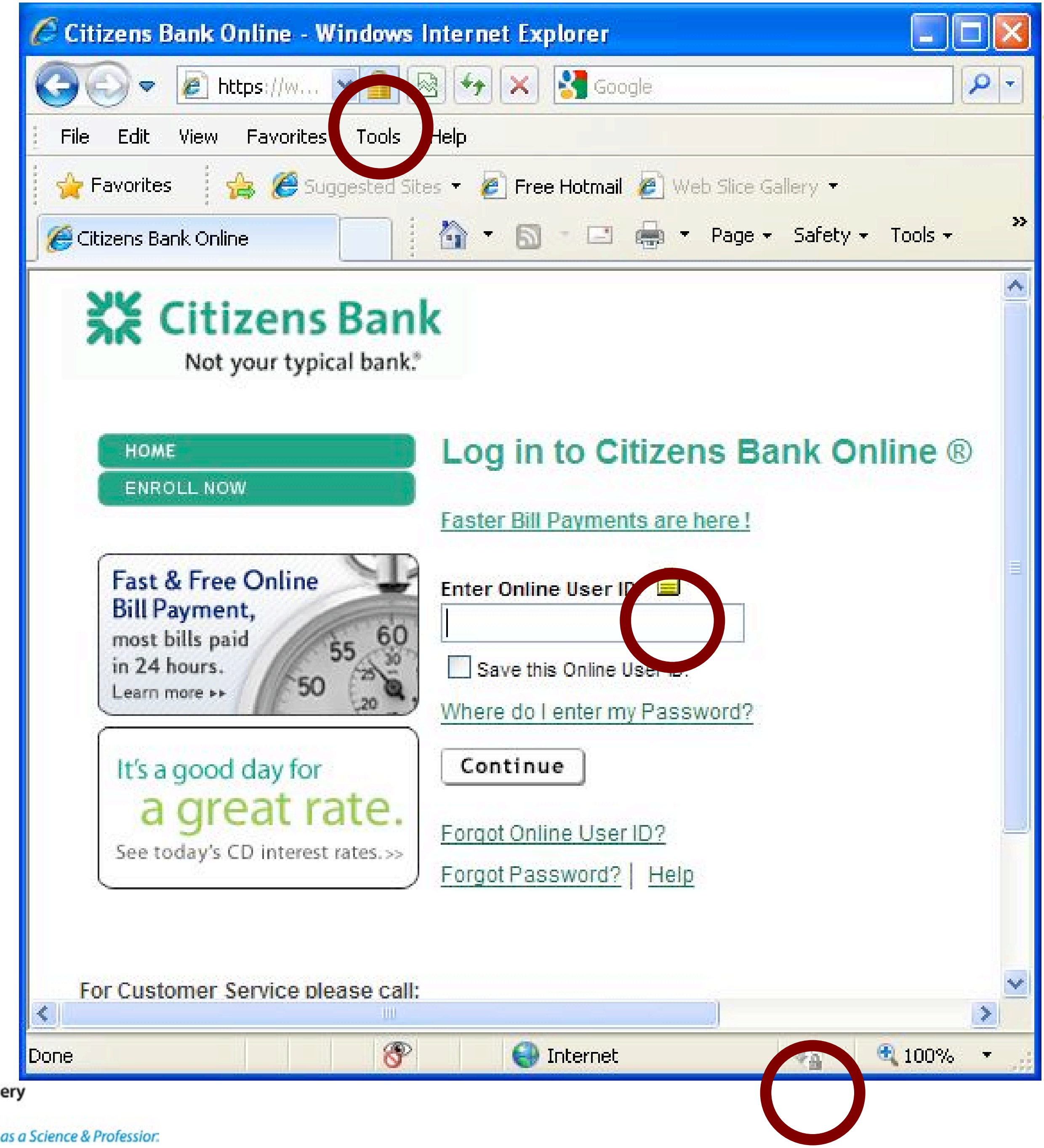
Trust

- “*reliance on the integrity, strength, ability, surety, etc., of a person or thing; confidence.*”- dictionary.com

- What is the role of trust in security?
- What does trust even mean?
- Can we move the social notions of trust into a technology context?

Usability

- End User:
  - How many passwords do you have?
  - How do you remember all your passwords?
  - Password must be 3,732 characters long and contain at least one upper case letter, one lower case letter, one digit and one special character.
  - "I've forgotten the password to the file where I keep all my passwords"
  - How do I know I'm secure online?
  - What does this error message mean?



Citizens Bank

Not your typical bank.®

HOME

ENROLL NOW

Fast & Free Online Bill Payment, most bills paid in 24 hours.

Learn more ▸▸

It's a good day for a great rate.

See today's CD interest rates.>>

Log in to Citizens Bank Online ®

Faster Bill Payments are here !

Enter Online User ID

□ Save this Online User ID.

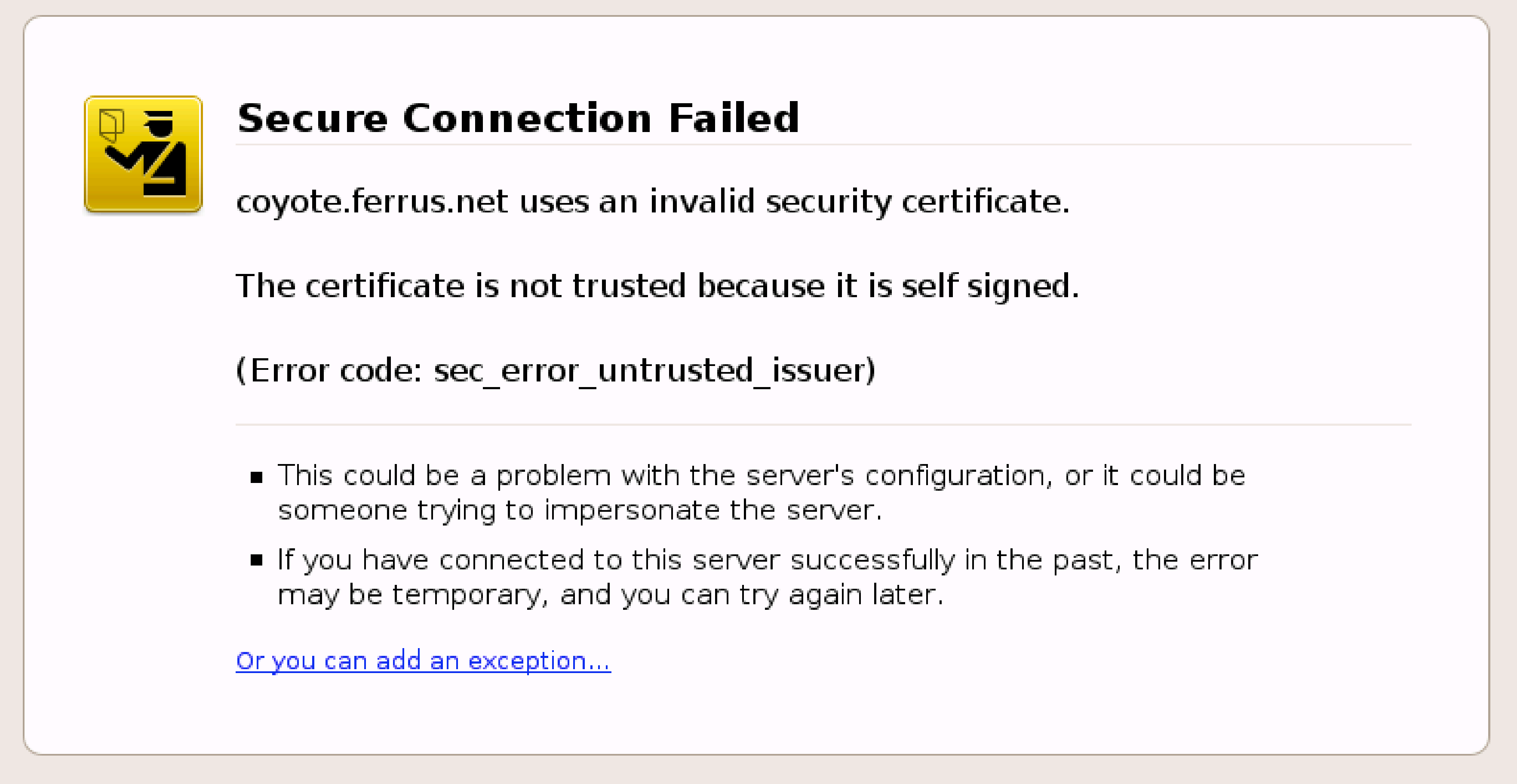
Where do I enter my Password?

Continue

Forgot Online User ID?

Forgot Password? | Help

For Customer Service please call:



Secure Connection Failed

coyote.ferrus.net uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_untrusted_issuer)

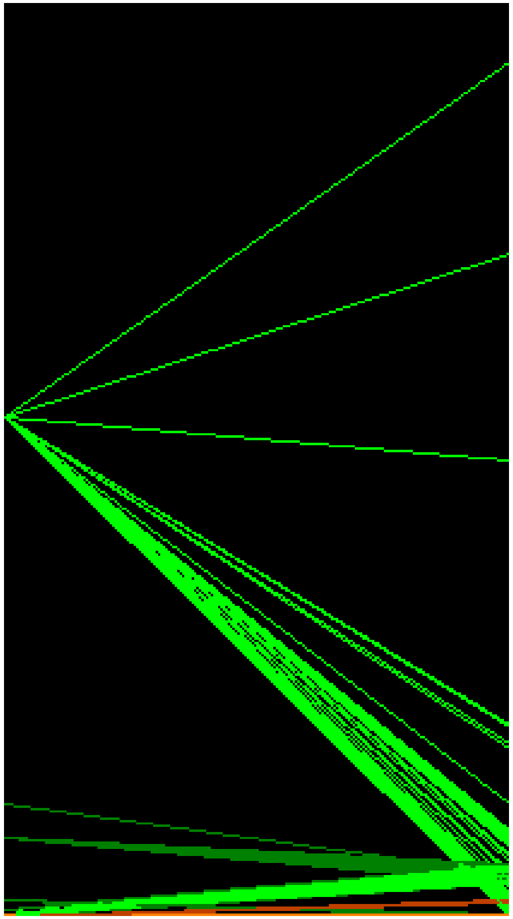
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

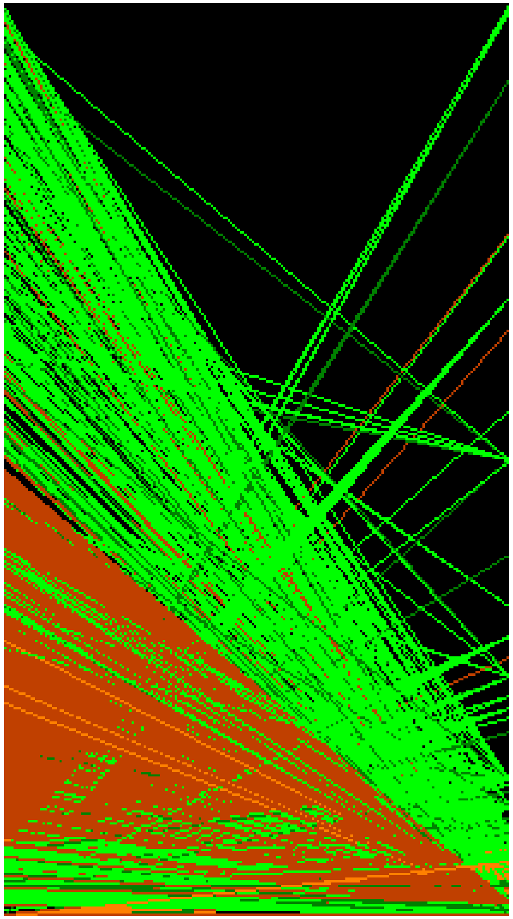
Or you can add an exception…

Usability

- End User:
  - How many passwords do you have?
  - How do you remember all your passwords?
  - Password must be 3,732 characters long and contain at least one upper case letter, one lower case letter, one digit and one special character.
  - "I've forgotten the password to the file where I keep all my passwords"
  - How do I know I'm secure online?
  - What does this error message mean?
- Security software itself

```
         sIP|          dIP|sPort|dPort|pro|   packets|     bytes|   flags|                  sTime|      dur|
168.192.2.25| 10.10.15.223| 1860| 2100|  6|         2|        96| S      |2006/07/03T19:23:15.000|    6.000|
168.192.2.25| 10.10.17.150| 2164| 2100|  6|         2|        96| S      |2006/07/03T19:23:25.000|    6.000|
168.192.2.25| 10.10.15.225| 2466| 2100|  6|         1|        48| S      |2006/07/03T19:23:35.000|    0.000|
168.192.2.25| 10.10.17.155| 3681| 2100|  6|         3|       144| S      |2006/07/03T19:24:12.000|    9.000|
168.192.2.25|  10.10.14.48| 3980| 2100|  6|         2|        96| S      |2006/07/03T19:24:25.000|    6.000|
168.192.2.25| 10.10.16.193| 3982| 2100|  6|         2|        96| S      |2006/07/03T19:24:25.000|    6.000|
168.192.2.25|  10.10.14.49| 4282| 2100|  6|         2|        96| S      |2006/07/03T19:24:35.000|    6.000|
168.192.2.25|  10.10.15.13| 4858| 2100|  6|         2|        96| S      |2006/07/03T19:24:45.000|    6.000|
168.192.2.25| 10.10.17.159| 1212| 2100|  6|         2|        96| S      |2006/07/03T19:24:56.000|    6.000|
168.192.2.25| 10.10.16.196| 1211| 2100|  6|         2|        96| S      |2006/07/03T19:24:56.000|    6.000|
168.192.2.25|  10.10.15.15| 1513| 2100|  6|         2|        96| S      |2006/07/03T19:25:06.000|    6.000|
168.192.2.25| 10.10.16.198| 1818| 2100|  6|         2|        96| S      |2006/07/03T19:25:16.000|    6.000|
168.192.2.25|  10.10.14.54| 2117| 2100|  6|         2|        96| S      |2006/07/03T19:25:26.000|    6.000|
168.192.2.25|  10.10.15.17| 2118| 2100|  6|         2|        96| S      |2006/07/03T19:25:26.000|    6.000|
168.192.2.25| 10.10.17.163| 2424| 2100|  6|         2|        96| S      |2006/07/03T19:25:36.000|    6.000|
168.192.2.25|  10.10.14.56| 2723| 2100|  6|         2|        96| S      |2006/07/03T19:25:46.000|    6.000|
168.192.2.25| 10.10.17.167| 3636| 2100|  6|         2|        96| S      |2006/07/03T19:26:16.000|    6.000|
168.192.2.25|  10.10.14.61| 4237| 2100|  6|         2|        96| S      |2006/07/03T19:26:37.000|    6.000|
168.192.2.25|  10.10.14.62| 4556| 2100|  6|         2|        96| S      |2006/07/03T19:26:47.000|    6.000|
168.192.2.25| 10.10.16.209| 1465| 2100|  6|         2|        96| S      |2006/07/03T19:27:07.000|    6.000|
168.192.2.25| 10.10.15.247| 1688| 2100|  6|         3|       144| S      |2006/07/03T19:27:07.000|    9.000|
168.192.2.25| 10.10.17.173| 1769| 2100|  6|         2|        96| S      |2006/07/03T19:27:17.000|    6.000|
168.192.2.25|  10.10.14.66| 1992| 2100|  6|         2|        96| S      |2006/07/03T19:27:21.000|    6.000|
168.192.2.25| 10.10.16.211| 2070| 2100|  6|         2|        96| S      |2006/07/03T19:27:27.000|    6.000|
168.192.2.25|  10.10.14.67| 2294| 2100|  6|         2|        96| S      |2006/07/03T19:27:31.000|    6.000|
168.192.2.25| 10.10.15.250| 2596| 2100|  6|         2|        96| S      |2006/07/03T19:27:41.000|    6.000|
168.192.2.25| 10.10.17.176| 2677| 2100|  6|         2|        96| S      |2006/07/03T19:27:47.000|    6.000|
168.192.2.25|  10.10.15.32| 2978| 2100|  6|         2|        96| S      |2006/07/03T19:27:57.000|    6.000|
168.192.2.25|  10.10.14.71| 3079| 2100|  6|         2|        96| S      |2006/07/03T19:27:59.000|    6.000|
168.192.2.25| 10.10.17.179| 3587| 2100|  6|         2|        96| S      |2006/07/03T19:28:18.000|    6.000|
168.192.2.25|  10.10.14.73| 3686| 2100|  6|         2|        96| S      |2006/07/03T19:28:19.000|    6.000|
168.192.2.25| 10.10.17.181| 4195| 2100|  6|         2|        96| S      |2006/07/03T19:28:38.000|    6.000|
168.192.2.25| 10.10.17.184| 1421| 2100|  6|         2|        96| S      |2006/07/03T19:29:08.000|    6.000|
```





Complexity

Adoption of Security Practices

- How many people here know all of the security policies for their organization?
- Now… how many of you adhere to all of them?

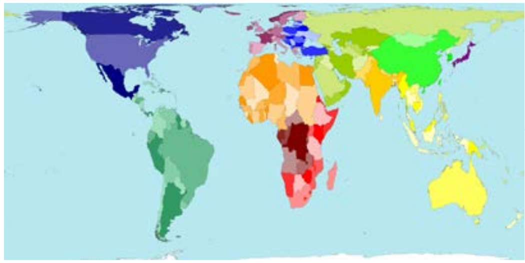
"I just want to be able to do my job!"

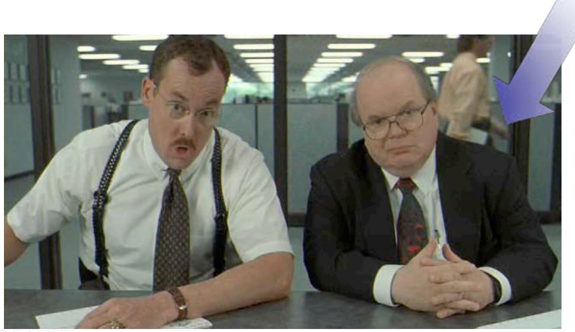
Security is the enemy!

Insider Threat

Insider Threat Examples

- Intentional Data Leaks
  - Malicious (e.g., Robert Hanssen, FBI)
  - Non-malicious (e.g., employees who looked at Obama’s cell phone records)
- Sabotage of Company Resources
  - IRS subcontractor Claude Carpenter inserted code on agency servers to delete their data
- Abuse of Privileges
  - Security supervisor at UK bank lets in 2 hackers, tries to steal £229 million
  - Joseph Colon, FBI: stole 38,000 employee passwords





My Definitions

- Insider:
  - “Insider with *respect to some resource or data*” (Dagstuhl 2008)
  - Restriction: “Insider *account* with respect to some resource or data” (Dagstuhl 2010)

- Perimeter:
  - Defined by what you can monitor
  - (Implications for outsourcing, SaaS, cloud….)

Masqueraders

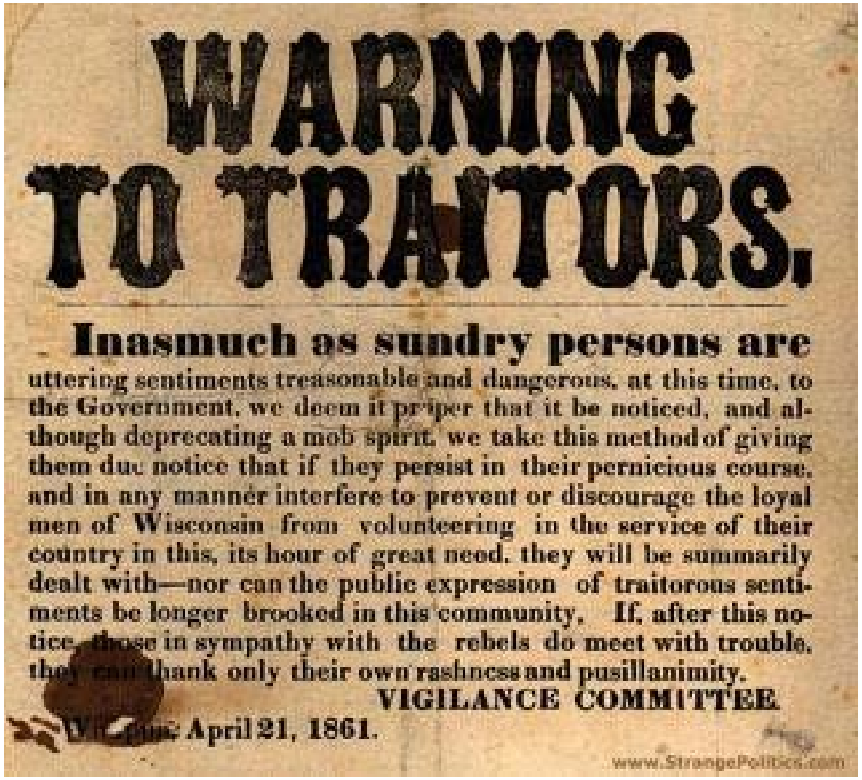
- Fundamental issue:
  - One person is trying to act like someone else
  - Goal: detect *attack*? Or detect that someone else has access to your account?
- Measure behavior
  - Unix commands, etc.
- Measure for X people
  - Are they different?
  - If one event is labeled as a different person, can it be detected?
- Is a masquerader an insider? ☺

Association for Computing Machinery

Advancing Computing as a Science & Profession

Traitors

- Fundamental issue: One person is intentionally doing something that violates policy (... Why? ...)
- Types of policy violations:
  - Malicious acts (e.g., planting a trojan horse, deleting files)
  - Leaking data
  - Abuse of privilege



WARNING TO TRAITORS.

Inasmuch as sundry persons are uttering sentiments treasonable and dangerous, at this time, to the Government, we deem it proper that it be noticed, and although deprecating a mob spirit, we take this method of giving them due notice that if they persist in their pernicious course, and in any manner interfere to prevent or discourage the loyal men of Wisconsin from volunteering in the service of their country in this, its hour of great need, they will be summarily dealt with—nor can the public expression of traitorous sentiments be longer brooked in this community. If, after this notice, those in sympathy with the rebels do meet with trouble, they can thank only their own rashness and pusillanimity.

VIGILANCE COMMITTEE.

Waupun April 21, 1861.

www.StrangePolitics.com

The Problem

- The traitor has legitimate access
- You are trying to infer *intent* from *actions*

Current Approaches

- Data Leak Prevention
  - Geared at *unintentional* loss of information
  - Requires manual tagging of information / regular expressions
  - Depending on monitor location, encryption is an issue
- Point Solutions
  - E.g., credit card fraud detection
  - Behavioral analysis at financial institutions

Like intrusion detection….

- Signature-based detection algorithms
  - How do you develop realistic signatures?
  - State of the art in industry are things like: X failed logins, or logging in at 3am, etc.
  - Does not necessarily distinguish between an “insider” and an “outsider”
  - But, assuming a half-way intelligent adversary….
- Anomaly-based detection algorithms
  - Standard assumption: there is a *normal* that can be modeled
  - Standard assumption: attack activity will appear as outside of normal activity (anomalous)

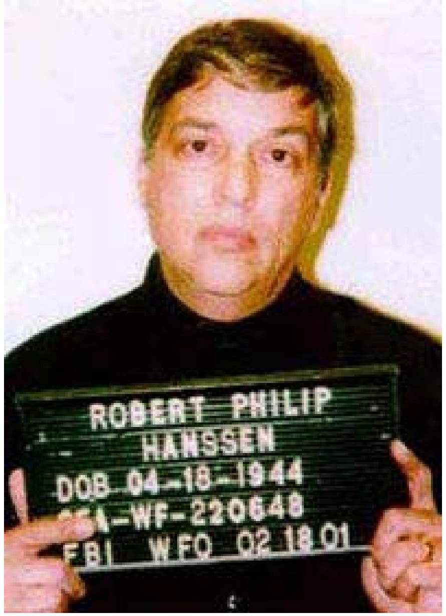
Data is King!

- What do insiders look like?
  - Have CERT studies and books on specific individuals, but paucity of hard data
  - Little technical data as in what actions, etc., *on the computer or network* distinguish them from non-insiders

- What data needs to be collected?
  - Anything that detects insider activity?! ☺
  - Data to detect data leakage different from syst attacks, for example

Unlike intrusion detection….

- Can marry transaction data with roles, identities, policies, etc.
  - Data is richer and more complex
- Person (account) might have legitimate access, so how do you tell *why* they are performing a particular action?
  - "Oracle" policies….
- How do you test your algorithm?



Insider Threat

- Identity, Trust, Usability, Adoption of Security

- Identity: Masquerader versus Traitor
- Trust
  - Who sees collected data?
  - False positives?
  - Privacy?
  - Does this inspire loyalty?
- Usability
  - Not just sys admins, all employees
- Adoption of Security

It’s all about people

Ultimately, how do you prevent insider attacks?

Happy employees

Conclusions

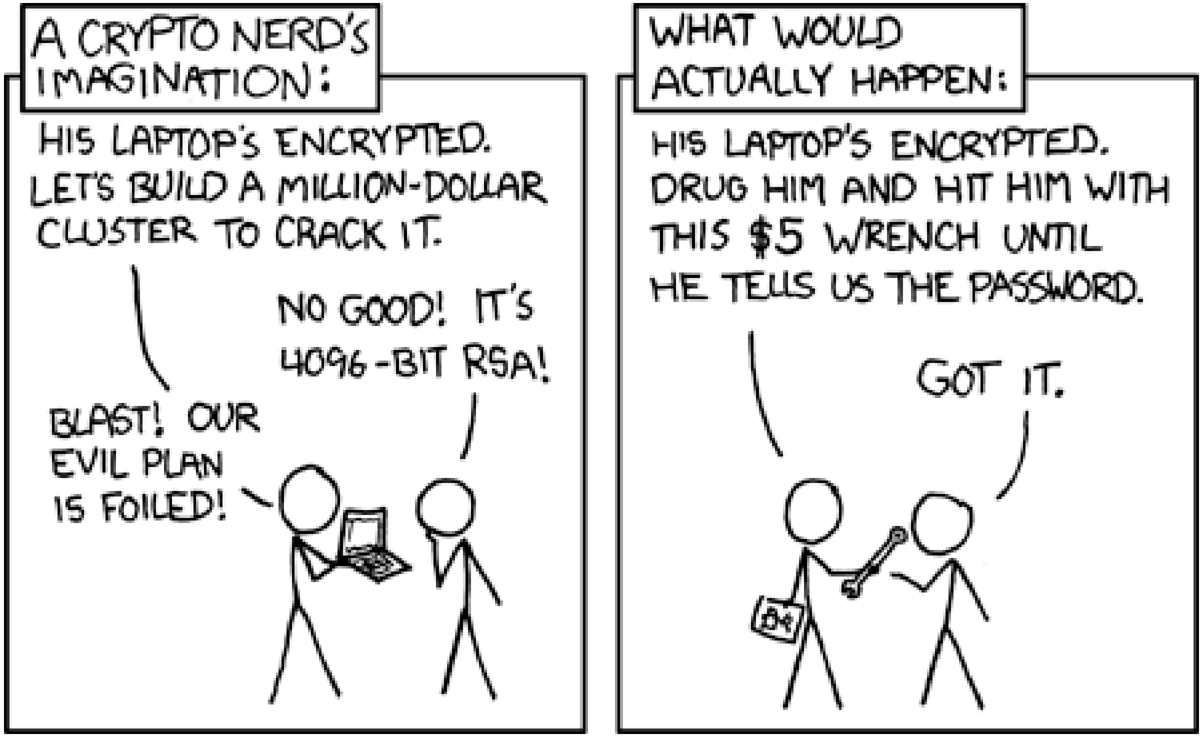
Why security is a special case

1. There's an adversary
2. The thought process around determining security is … different
3. The concepts can be difficult concepts - how do you teach them?
4. It's a feature, not the main functionality
5. There can be a large amount of complexity
6. Security operates at multiple levels: end user, admin, organization
7. How do you know the “who” in, e.g., an attack?
8. There is generally considered to be a trade-off between usability and security
9. How do you test security? Experiments on users might not be ethical….
10. Trust is important, but how do you generate trust?

Association for Computing Machinery

Advancing Computing as a Science & Profession

The Truth….


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
$4

Mouse-over:
Actual actual reality: nobody cares about his secrets. (Also, I would be hard-pressed to find that wrench for $5.)

http://xkcd.com/538/

Association for Computing Machinery

Advancing Computing as a Science & Profession

ACM: The Learning Continues

- Questions about this webinar? learning@acm.org
- ACM Learning Center: http://learning.acm.org
- USACM Public Policy Council (Privacy & Security): http://usacm.acm.org/privsec/
- ACM SIGSAC: http://www.sigsac.org

Association for Computing Machinery

Advancing Computing as a Science & Profession

Microsoft Research