Summary

• Myth #1: statistics
• Myth #2: passwords
• Myth #3: random number generators
• Myth #4: master keys
• Myth #5: mobile/embedded/SCADA
• Myth #6: BYOD
• Myth #7: TPM
• Myth #8: China
• Myth #9: cloud
• Myth #10: privacy
Myth #1: Statistics

Verizon 2012 Data Breach Investigation Report: 58% of data stolen in 2011 was the result of hactivism, which involves computer break-ins for political rather than commercial gain.

In previous years, most hacking was carried out by criminals.

Myth #1: Statistics

FUD

Lies, damned lies, and statistics
How big is cybercrime: recent estimates

E. Amoroso, CSO, AT&T

Approximately 1 trillion $

Kilian Strauss (OSCE)

Annually

100 billion $

SSG-Inc.

Annually

10 billion $

P. Peterson, Cisco Fellow

Annually

0.56 billion $

Sex and Lies

Men claim from 3..9 times more lifetime heterosexual partners than women

Morris [Nature'93] “male reports only slightly exceed female reports for lower 90% of the sample, but dramatically exceed them for the upper 2%”

<table>
<thead>
<tr>
<th></th>
<th>Male/Female reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>3.2</td>
</tr>
<tr>
<td>Bottom 90%</td>
<td>1.2</td>
</tr>
<tr>
<td>Top 10%</td>
<td>10.1</td>
</tr>
</tbody>
</table>
So how can this be?

- Consider man with 2x overstatement
  - Correct answer is 50 but claims 100
- Takes 16 men at the median level to understate by a factor of 2 to cancel out this error
- Problematic for uneven distribution with small number of outliers

Cybercrime surveys

Mean/median > 3: tiny fraction of respondents account for majority of estimate

<table>
<thead>
<tr>
<th></th>
<th>Mean/Median</th>
<th>Top 1% accounts for</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Wealth</td>
<td>4.1</td>
<td>33%</td>
</tr>
<tr>
<td>FTC ID Theft 2006</td>
<td>3.8</td>
<td>30%</td>
</tr>
<tr>
<td>Gartner Phishing 2007</td>
<td>4.5</td>
<td>59%</td>
</tr>
<tr>
<td>DoJ Theft Survey 2008</td>
<td>9.3</td>
<td>72%</td>
</tr>
<tr>
<td>IC3 ID theft 2007</td>
<td>9.7</td>
<td>78%</td>
</tr>
</tbody>
</table>
How big is cybercrime?

E. Amoroso, CSO, AT&T

Approximately 1 trillion $

we don’t know
ask for the median

Source: Dinei Florencio, Cormac Herley, Sex, Lies and Cybercrime Surveys. Microsoft Research, 2011

Myth #2: Passwords

Bill Gates: 2004: Passwords are dead

• But today most of us have 30-40…

• Cheap and easy to reset
• Insecure: guess, intercept, reuse….
• Countermeasure: (crazy) password policies
  – complex rules: U8rM@4IoW9
  – expire after 90 days
  – never write them down

Users and IT security people universally hate passwords
Myth #2: Passwords

• Attack vectors
  – Key stroke logging
  – Phishing
  – Guessing/brute-forcing
  – Shoulder-surfing
  – Session high-jacking

• Hierarchy of risks
  – Health/bank/employee accounts
  – Merchant and retail
  – Email/social networks
  – Newspaper
  – WiFi

• How to quantify harm?
• Monetizing stolen passwords is non-trivial

Complex ecosystem: incentives?

Replacing passwords?
• inertia: who goes first?
• which technology
• who pays?
• risk of integrated system

• Open ID
• Cardspace
• …
Myth #2: Passwords

Passwords are not dead! They need more research

- Better understanding of risks/threats
- Password aging policies
- Realistic user guidance
- Password managers (malware, roaming,…)

Source: C. Herley, P.C. van Oorschot, A Research Agenda Acknowledging the Persistence of Passwords

Myth #3: Random Number Generators

Trust us. We know what we are doing

- 1995: Netscape SSL problem
- 2006: Linux
- 2007: Microsoft Windows
- 2008: OpenSSL keys: Debian Problem
- 2010: Sony Playstation 3: ECDSA Problem
- 2011: Problems with RNGs in virtual machines

- More technical stuff
  - 2001 Bleichenbacher DSA –FIPS 186
  - 2003 Phong Nguyen GPG
RSA key pairs: “Ron was wrong, Whit is right”

- 11.7 million openly accessible public keys
- 6.4 million distinct RSA moduli
- rest: ElGamal/DSA (50/50) and 1 ECDSA

- 1.1% of RSA keys occur in >1 certificate
- 0.2% (12934 moduli) are easy to factor, because they form pairs e.g. \( n = p \cdot q \) and \( n' = p' \cdot q \) so \( \gcd(n, n') = q \)
  - 40% of these have valid certs
  - reason: only 40-bit randomness in key generation combined with the birthday paradox
- less of a problem for ElGamal/DSA: need to know how randomness is produced and complexity is \( 2^{40} \) key generations
- ethical problem: how to report this?

Read more: A.K. Lenstra et al. “Ron was wrong, Whit is right”
http://print.iacr.org/2012/064.pdf

Myth #3: Random Number Generators

NIST will broadcast a randomness beacon (not secret obviously)

Intel will offer a 2 Gbps RNG in every high end chip (Bull Mountain)

Whose random number generator do you trust?
Myth #4: My Cryptographic Master key is Secure. It is Stored in an HSM

- Crypto moves problems to keys 🚧 🚧 🚧
- The world becomes simpler if we only have to protect a small set of super important master keys

- Indeed

Just ask Diginotar, Comodo, RSA

..or the Government of Malaysia that signed malware
Myth #4: My Cryptographic Master key is Secure. It is Stored in an HSM

Distributed cryptography has the potential to be more robust

Myth #5: Hacking mobile/embedded/SCADA systems is difficult

- A5/1 weak
  - [Barkan+03] requires seconds (software not available so requires math)
  - [Nohl10]: Kraken = 2 Terabyte of Rainbow tables
    http://reflextor.com/trac/a51
- A5/2 trivially weak (milliseconds) – withdrawn in 2007 (took 8 years)
- A5/3 (= Kasumi) seems ok but slow adoption (even if in 1.2 billion out of 3 billion handsets)

- simpler attacks on GSM
  - eavesdrop after base station (always cleartext)
  - switch off encryption (can be detected)
  - SMS of death
GSM

- growing number of open source tools to intercept: GnuRAdio, Airprobe, OpenBTS
- but needs more work (1-2 years?)

GSM

- be careful when rolling out 2-factor authentication via SMS
- war texting hacks on car systems and SCADA systems [Black Hat, Aug’11]
**Wireless hacks abound**

- Police radio: APCP Project 25 [Clark+11]
- Car electronics: now wireless [Checkoway+11] or via MP3
- Electronic car lock denial of service attack
- iPhone encryption
- Keylogger in drone command & control center
- Flying drones for hacking
- Plug Bot

---

**Embedded webservers**


Zscaler lab: bREWS tool to test embedded web servers in digital scanners, office printers, VoIP systems, storage devices, …

**SCADA**

Second water utility reportedly hit by hack attack. Water pump broken (18/11/2011)
Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System
Myth #6: BYOD (was: consumerization)

**BYOD is under control**

- **Bring Your Own Device or Bring Your Own Danger?**

- some statistics (but remember Myth #1)
  - 75% of IT professionals believe that personally owned mobile devices put their organizations at risk
  - 39% have the necessary security controls to address the risk
  - 59% report that employees circumvent or disengage security features, such as passwords and key locks

---

Myth #6: BYOD (was: consumerization)

- **Issues**
  - mixing corporate and personal data
  - what if person leaves the organization
  - large percentage of employees use DropBox

- Need to give access to corporate data without the ability to scrape it, send it or save it – this is the DRM problem
- Monitor rather than forbid
- Hope for the best...

**Solution: 85% policy + 10% technology**
Myth #7: China

China is a growth opportunity for IT security

- Every cryptographic algorithm used in China has to be designed in China
  - examples: SMS4, ZUC,…
- WAPI for wireless LAN – mandated for smartphones
- April 2009: 13 categories of IT security products should conform to the CCC (China Compulsory Certificate) = Chinese version of the “Common Criteria”
- 110 information security standards under development (http://www.tc260.org.cn)

Myth #8: TPM

TPM improve the security of our devices

- Cryptographic processor with secure key storage and random number generation
  - secure boot
  - access control
  - device authentication and attestation
  - disk encryption
  - DRM and licenses
  - VPN/wireless
- 500 Million PCs have shipped with a TPM chip
  - number of activated TPM chips = ???
Myth #8: TPM

Malware can also use TPM to protect itself

- Malware can use TPM to receive encrypted code and preclude static and dynamic analysis
- Would need help of TPM vendor or hardware attack on TPM to bypass this protection


Myth #9: Cloud

The cloud will make us more secure

- Define?
  - private/community/hybrid/public
  - SaaS, PaaS, IaaS
- Reduce capital and operational expenses
- Scalable and elastic architecture
Is the cloud more secure?

- What’s the same
  - can do intrusion detection/monitoring
  - can encrypt stored data – but key management problem
  - availability? Service/network/power – SLA

- What’s different
  - VM sprawl
  - AV/firewall could improve (e.g. availability)
  - pen testing
  - forensics
  - personnel security: separation of duty management of privileges for people and...

Is the cloud more secure?

- Availability
  - the hidden risk of a meltdown in the cloud
  - clouds can evaporate

  April 21, 2011, Amazon EC2 outage downs Reddit, Quora
  January 19, 2012, Megaupload Taken Down On Piracy Allegations
  March 2, 2012 Windows Azure Leap-Year Glitch Takes Down G-Cloud

- Privacy

- Large and attractive target
  - What if someone takes over the infrastructure management?
Myth #10: Privacy

We can keep control over our private data, as long as we are careful

• Facebook tracks users even if logged out – even non-Facebook users
• P2P traces TOR users [LeBond et al. Usenix LEET11]
• Speaker recognition from encrypted VoIP [Khan-Baig-Youssef]
• Target discovers that women are pregnant before they know themselves
• Facebook + face recognition = the end of privacy? [Acquisti]
• Cloud has been transformed into BIG DATA

The end

Thank you for your attention

Bart.Preneel(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel