Cyber Security: What You Need to Know

Prof. Ravi Sandhu
Executive Director and Chief Scientist
Institute for Cyber Security
University of Texas at San Antonio
October 2009

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu

99-1 Principle (Roughly)

99% of the attacks are thwarted by basic hygiene and some luck

DO

- Think before you click etcetera
- Up-to-date anti-virus, firewall and site advisor

BUT

- Some new attacks may get through. However, attacker may only use your machine to attack others and not attack you per se.
- Will not prevent data loss by merchants and other servers. However, still have safety in numbers. Attackers can steal a lot of account numbers but can exploit much fewer.

1% of the attacks are difficult and expensive to defend or detect

For most individuals

- We are simply not an attractive enough target.

For the US Department of Defense and its contractors

- A huge target. Current score: 50-1 in favor of attackers (roughly)

For companies in less sensitive businesses

- A serious threat to be taken seriously

Weakest Link: Password Reset

Typically done via secret questions and email to preferred email account

- Mother's maiden name?
- Father's middle name?
- Favorite pet's name?
- etcetera

- *"As detailed in the postings, the Palin hack didn't require any real skill. Instead, the hacker simply reset Palin's password using her birthdate, ZIP code and information about where she met her spouse — the security question on her Yahoo account, which was answered (Wasilla High) by a simple Google search."*

Password reset on preferred email account itself done via secret questions

Conundrum

- Real answers easy to remember but discoverable via Google
- False answers hard to remember but safe from Google

Crystal Ball: In the Year 2025

PRIVACY

- Expectation (and delivery) of privacy is close to zero

E-COMMERCE SECURITY

- Close to perfect

NATIONAL AND CORPORATE SECURITY

- The nation-state threat should be better contained
- The asymmetric non-nation-state threat will remain

Crystal Ball: In the Year 2025

PAST, PRESENT

- Cyber security is a young and immature field
- The attackers are more innovative than defenders
- Defenders are mired in FUD (fear, uncertainty and doubt) and fairy tales
- Attack back is illegal or classified

FUTURE

- Cyber security will become a scientific discipline
- Cyber security will be application and technology centric
- Cyber security will never be “solved” but will be “managed”
- Attack back will be a integral part of cyber security

Cyber Security: Major Trends

Security Objectives:

- Black-and-white to shades of grey

Attackers:

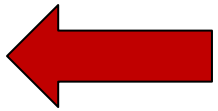
- Innovative beyond belief

Defenders:

- Need new doctrine

Cyber Security: Major Trends

Security Objectives:



- Black-and-white to shades of grey

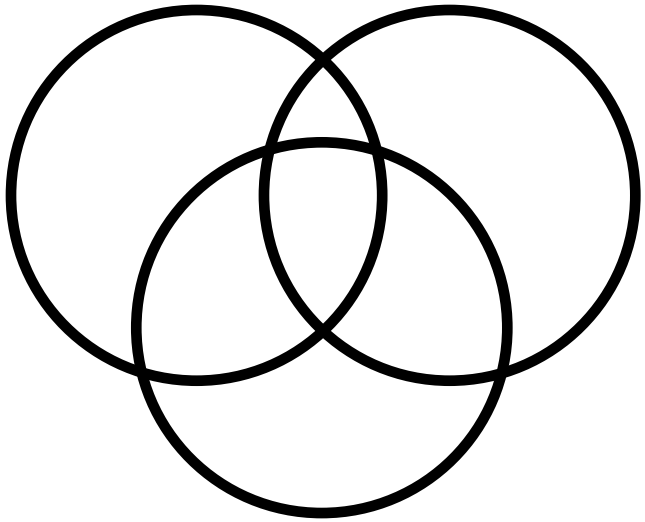
Attackers:

- Innovative beyond belief

Defenders:

- Need new doctrine

Cyber Security Objectives

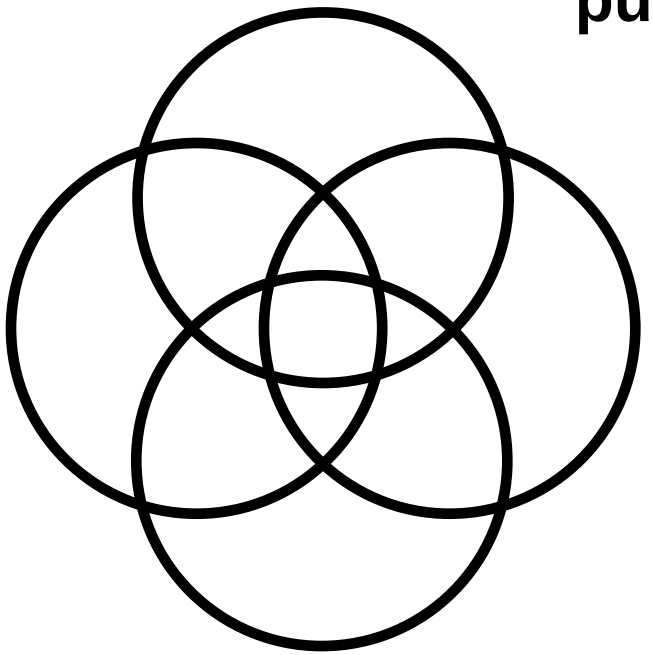


INTEGRITY
authenticity

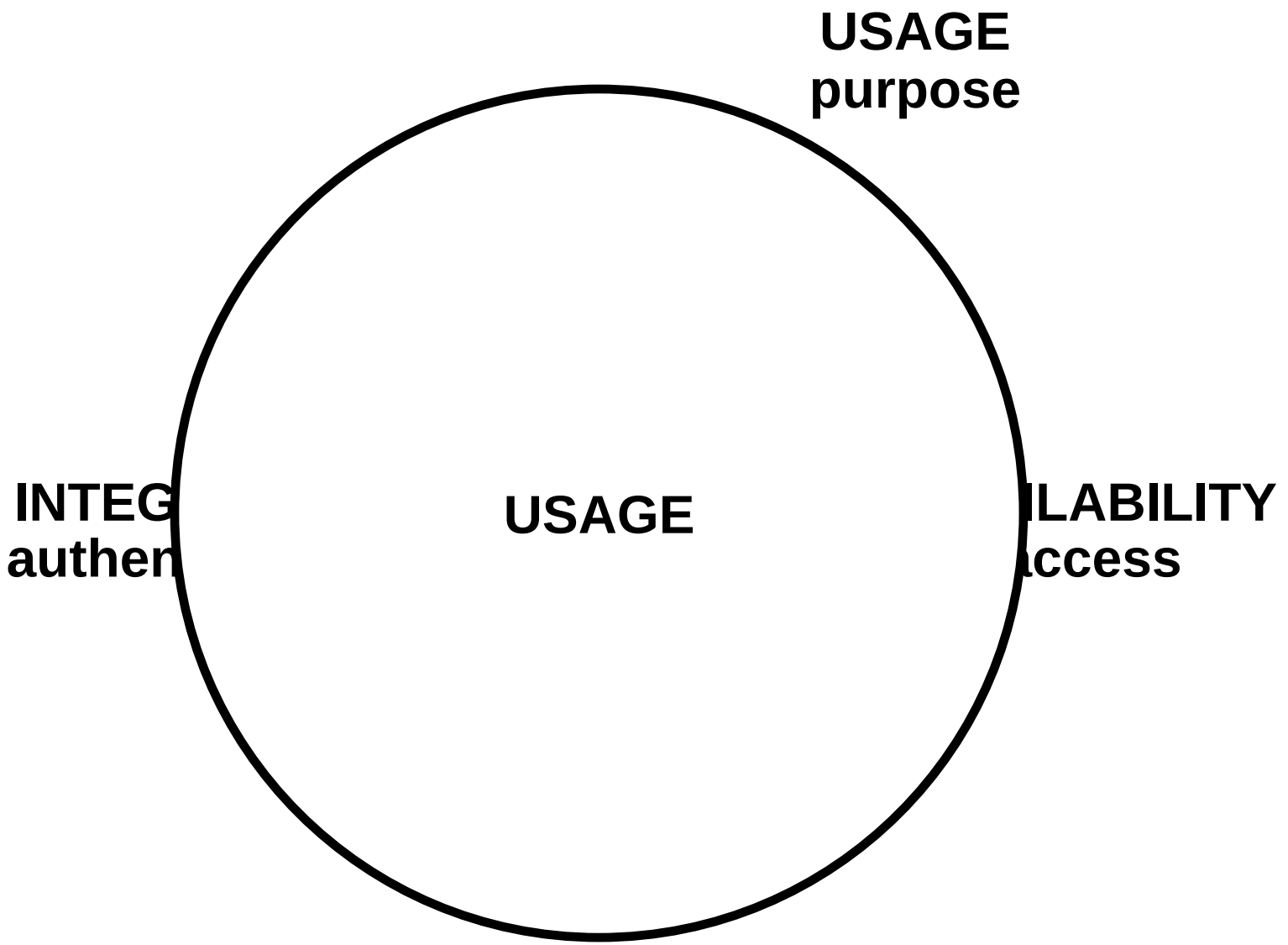
AVAILABILITY
access

CONFIDENTIALITY
disclosure

Cyber Security Objectives



Cyber Security Objectives



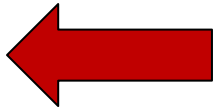
Cyber Security: Major Trends

Security Objectives:

- Black-and-white to shades of grey

Attackers:

- Innovative beyond belief



Defenders:

- Need new doctrine

Attackers: Innovative Beyond Belief

Major Innovations

- Botnets
- Robust underground economy and supply chain
- Targeted attacks
- Stealthy attacks

Some Examples

- Drive by downloads
- Scareware
- Doctored online statements
- Long-lived stealth attacks

Status

- Attackers have sizable inventory of known but unused or rarely used tricks
- Innovation will continue

Cyber Security: Major Trends

Security Objectives:

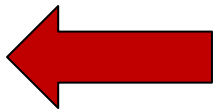
- Black-and-white to shades of grey

Attackers:

- Innovative beyond belief

Defenders:

- Need new doctrine



Defenders: Need New Doctrine

- OLD: Cyberspace is a supporting infrastructure
- NEW: Cyberspace is a war-fighting domain on par with land, sea, air and space

- OLD: It's all defense, no attack back or preemptive attack
- NEW: All's fair in war

- OLD: Defend the entire network to the same degree
- NEW: Defend selectively and dynamically

- OLD: Blame and harass the end user
- NEW: The user is part of the solution

- OLD: Defend against yesterday's attacks
- NEW: Be proactive, get ahead of the curve, future-proof

Institute for Cyber Security (ICS)
Founded 2001

Research Excellence

- Secure Information Sharing
- Social Computing Security
- Cloud Computing Security
- Malware Mitigation
- Military Grade Security
- Infrastructure Assurance and Security

50+ people and growing

A jewel in UTSA's drive to tier I status

Research Laboratories

- FlexCloud: cloud platform
- FlexFarm: malware honeyfarm
- Community exercises: the real real-world

Core Differentiators

- We are the flagship for cyber security research at UTSA
- We are unique amongst the myriad academic cyber security centers in the country due to our demonstrable emphasis on real-world impact