

Scaring You Secure

Welcome to the (IT) jungle...

By Marc DeBonis

OS Analyst

IS&C – Virginia Tech

What is security?

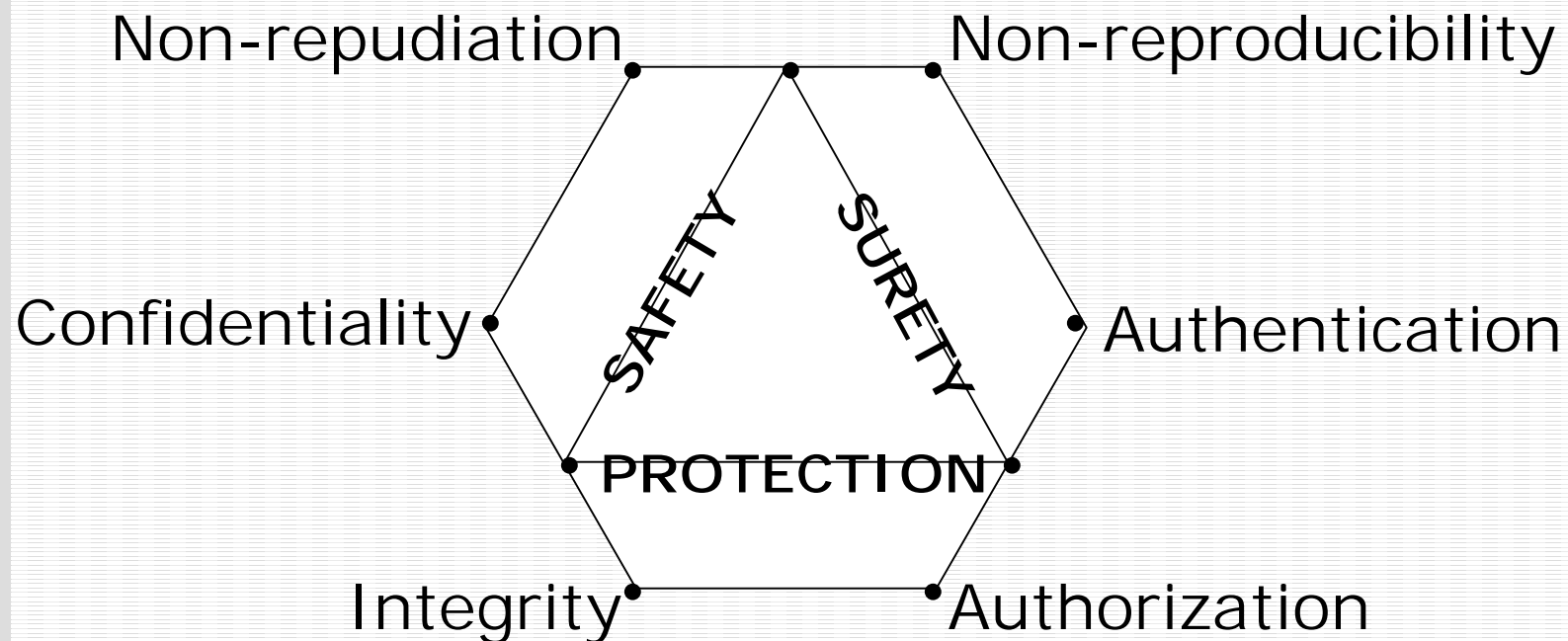
- Merriam-Webster's Collegiate Dictionary
 - Main Entry: se•cu•ri•ty
 - Pronunciation: si-'kyur-&-tE
 - 1. The quality or state of being secure: as
 - a: freedom from danger : SAFETY
 - b: freedom from fear and anxiety
 - c: freedom from the prospect of being laid off
 - 2.
 - a: something given, deposited, or pledged to make certain the fulfillment of an obligation : SURETY

What is security?

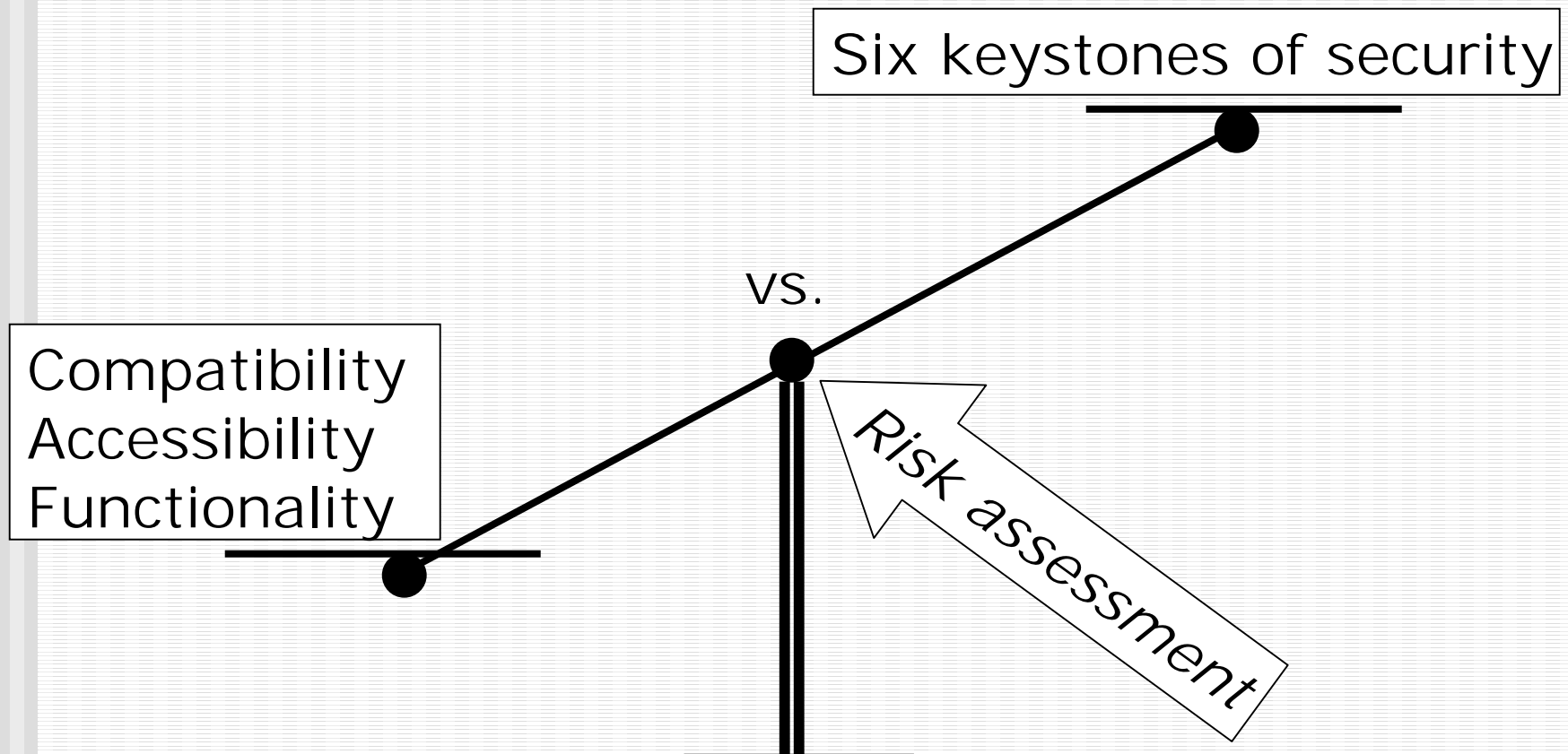
- Merriam-Webster's Collegiate Dictionary
 - 3. An evidence of debt or ownership
 - 4.
 - a: something that secures : PROTECTION
 - b:
 - 1: measures taken to guard against espionage or sabotage, crime, attack, or escape
 - 2: an organization or department whose task is security

Security in IT

- Six keystones of security



The "versus" scale



Why should you care?

- The bottom line = \$\$\$
 - Risk assessment to loss of systems
 - What is the \$/hr for a end user workstation
 - What is the \$/day for a server
 - What is the \$/week, month, year for a critical system
- Worst case
 - Production Banner goes down and never comes back

Why should you care?

- Liability = responsibility
 - State and federal guidelines for IT data, systems and security
 - What would be the legal ramifications if somebody broke in and stole all Faculty, Staff and Students SSNs? CC #s from online learning courses? Email addresses for spam?
- Worst case
 - System insecurity leads to a leak of confidential information which results in a very big lawsuit

Why should you care?

- Damages prestige of the University
 - Bad press directly/indirectly influences:
 - Faculty, students, staff and alumni
 - *Potential* faculty, students and staff
 - Causes us to become a known target
 - Weak security = easy target
 - Word gets around *VERY QUICKLY* in hackerdom
- Worst case
 - *New York Times* front page article deriding you, your department and the University

Why should you care?

■ AUP (acceptable use policy)

Guidelines

In making acceptable use of resource you must:

- protect your userid and system from unauthorized use. You are responsible for all activities on your userid or that originates from your system.

■ Worst case

- You have 10 minutes to clear out your desk...

The big fallacy

- “There's nothing on my computer anybody would want!” – anon IT manager
 - Would you want everyone/anyone to:
 - Look at the web sites you've visited?
 - Read all your email?
 - Write email with your userid?
 - Use any credit cards you've used online?
 - Alter/delete data on your system?
 - Hijack your system for further attacks to other systems?

True horror stories

- .edu web sites defaced
 - <http://www.attrition.org/mirror/attrition/edu.html>
- Macro virii
 - "ILOVEYOU" virus -- worldwide impact
 - Losses in North America estimated > **\$1 billion**
 - Inconvenient to devastating impact
 - Cluttered e-mail in-boxes, overloaded IS personnel
 - Web site crashes, lost e-commerce revenue, corrupted data
- Trojan attachments (Netbus, BO2k)
 - Loss of "Ownership" of a system

Types of attacks

- Physical
 - Lowest paid employees have greatest accessibility to our systems
- Social
 - People tend to trust people
 - The golden rule vs. the brass rule
- Network
 - What you can't see can hurt you

Physical

■ Attack

- People paid to look the other way, theft
 - >\$120 billion loss in employee fraud for 2000
- Disgruntled ex-employee/spouse
- Distractions for support staff (sugar in tank)

■ Defend

- Encrypt the system and laptops
- Do secure remote backups
- Use biometric identification
- Look up ↑ (drop down ceilings)

Social

- Attack
 - Giving false credentials to reset password
 - Forged email, trojan attachment
 - 37% of people surveyed would read email entitled "ILOVEYOU" and launch the attachment
 - Claim from help desk, get root on desktop
- Defend
 - Do not give passwords over the phone
 - Exit interview, removal of authorization
 - Challenge strangers for ID
 - Do callback to main number for verification
 - Sign email, do not allow attachments

Network

- Attack
 - Eavesdropping
 - Data modification
 - Identity spoofing
 - Password based attack
 - Denial of service (DoS)
 - Man-in-the-middle
 - Compromised key attack
 - Sniffer attack
 - Application-layer attack

Network

- Defend
 - Ipv6 (Internet Protocol Security)
 - Protects on a IP packet level
 - Encrypts data
 - Checksum data
 - Does key exchange verification
 - Do not allow non-job/untrusted applications
 - Harden passwords or use biometrics
 - Proactive scanning of subnets, security audits
 - Enforce security policies regardless of status
 - Do not give users administrative rights

In conclusion

- Security
 - Is like an onion
 - The more layers a hacker is required to peel, the more like they're liable to cry and move on
 - Should not be an afterthought
 - If it's not designed in, it's tacked on
 - Should be proactive, not retroactive
 - Better to do fire prevention than smoke inhalation

Recommendations

- Develop a tightly knit, proactive IT security group not beholden to any current informational or operational group with the necessary political power to get things done
- Develop a homogenous, secure and robust hardware and software platform
- Bring security to the forefront in people's minds and make a serious, concerted and continuous commitment to provide VT with a safe, sure and protected computing environment

Scaring You Secure

Welcome to the (IT) jungle...

By Marc DeBonis

OS Analyst

IS&C – Virginia Tech

• • •

- Welcome to the jungle We've got fun 'n' games We got everything you want Honey, we know the names We are the people that can find Whatever you may need If you got the money, honey We got your disease CHORUS: In the jungle Welcome to the jungle Watch it bring you to your knees, knees I wanna watch you bleed Welcome to the jungle We take it day by day If you want it you're gonna bleed But it's the price you pay And you're a very sexy girl That's very hard to please You can taste the bright lights But you won't get them for free In the jungle Welcome to the jungle Feel my, my, my serpentine I, I wanna hear you scream Welcome to the jungle It gets worse here everyday Ya learn ta live like an animal In the jungle where we play
- If you got a hunger for what you see You'll take it eventually You can have anything you want But you better not take it from me CHORUS And when you're high you never Ever want to come down, YEAH! You know where you are You're in the jungle baby You're gonna die In the jungle Welcome to the jungle Watch it bring you to your knees, knees In the jungle Welcome to the jungle Feel my, my, my serpentine In the jungle Welcome to the jungle Watch it bring you to your knees, knees In the jungle Welcome to the jungle Watch it bring you to your It' gonna bring you down-HA!
- © Guns N' Roses 1987