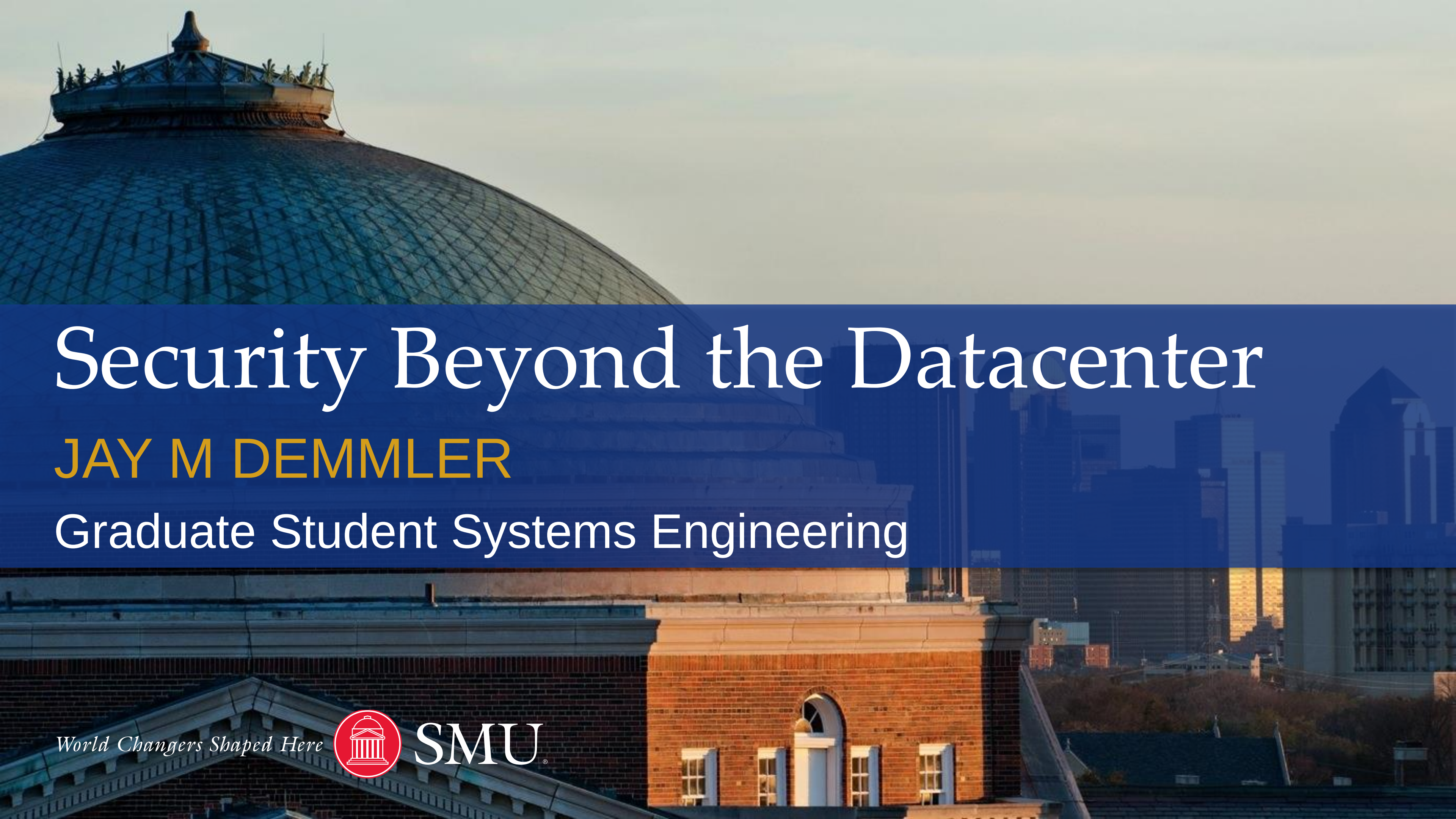
Jay Demmler is a graduate student of engineering at the Lyle School of Engineering at Southern Methodist University in Dallas, Texas. Jay previously received his BS from The University of Akron in Ohio. He then moved to Texas to work for Lockheed Martin on the F-35 Joint Strike Fighter project where he worked on designing and implementing enterprise systems for parts and services subcontractors. After a 2 year deployment abroad working on defense projects in Kuwait and Afghanistan, Jay moved back to the Dallas area to work for Dell Computer's services division (formerly Perot Systems). There he worked on a range of projects in the healthcare industry focusing on designing enterprise class systems in healthcare finance for Medicaid. Medicare, payer. and the revenue cycle industries. Jay is a frequent speaker and guest lecturer in the Dallas area where he often speaks to Systems Development Life Cycle, data center security and best practices, and IT transformation. His current research interests are STEM success rates at the Community College level, the use of asymmetrical learning tools in higher education, and efficiency and best practice development for enterprise class systems. Jay lives in Allen, TX with his lovely wife and two very large cats.



Security Beyond the Datacenter

JAY M DEMMLER

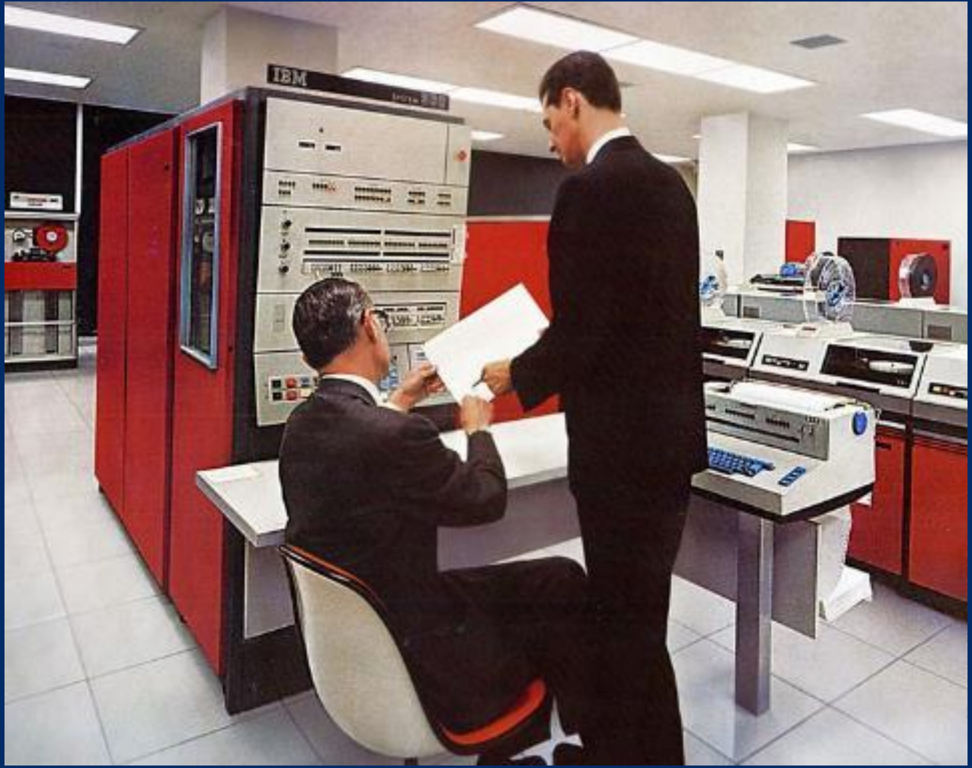
Graduate Student Systems Engineering

World Changers Shaped Here SMU

So what are we afraid of?

- Distribution of hoax emails
- Accessing unauthorized computers
- Engaging in data mining via spyware and malware
- Hacking into computer systems to illegally access personal information, such as credit cards or Social Security numbers
- Sending computer viruses or worms with the intent to destroy or ruin another party's computer or system

A long time ago…



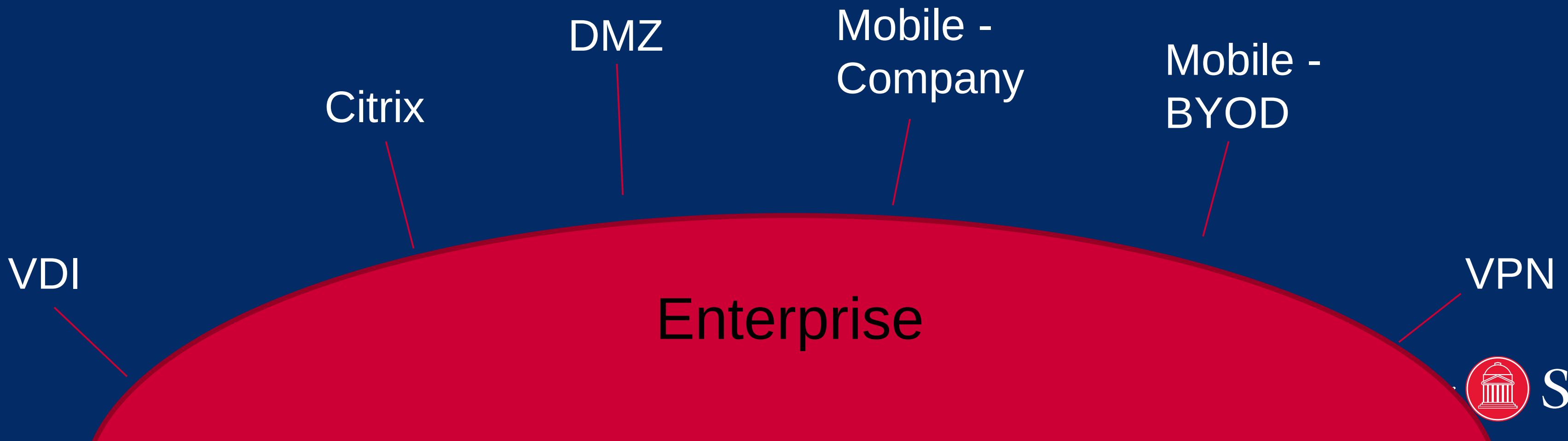
Access has evolved over time

- In ancient history (before 1980’s) few individuals had access to electronic data within a corporation
- Data Fraud would consist of individuals physically removing media or printouts from the datacenter
- As PC prices plummeted more and more users gained access to corporate networks
- Add in the shrinking of media storage forms and your risks rise again

Access has evolved over time cont.

- With the advent of cheap high speed internet to the home and a drop in laptop prices, VPN connectivity took off
- Then the Blackberry became synonymous with business
- And finally we now have powerful smart phones as well as BYOD connecting into our organizational networks

Vulnerability Threshold©



VDI

Citrix

DMZ

Mobile - Company

Mobile - BYOD

VPN

Enterprise

So What’s the Big Deal?

- To meet business needs access and data have proliferated outside the traditional walls of the organization
- Each new access method increases risks as it opens an additional opportunity for malicious exploitation
- While all vulnerabilities need to be addressed, some may require extra care to meet both business needs and the sensitivity of the data

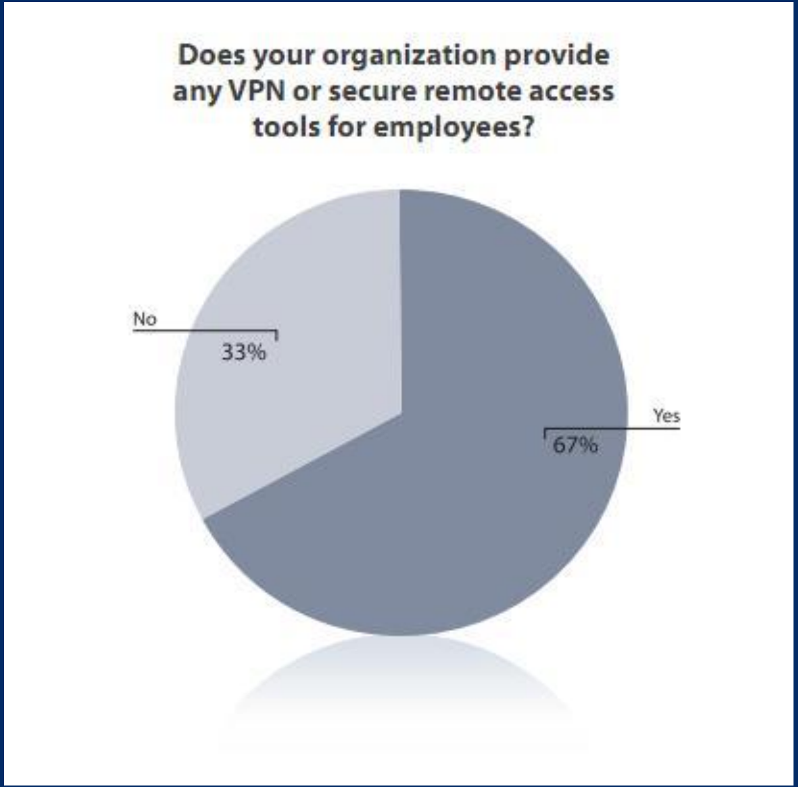
Laptops & Mobile Computing

- Small incremental cost of laptops over a traditional desktops have allowed businesses to deploy them almost exclusively
- Portable, powerful, and allowing for that always “on the clock” employee
- Thousands of laptops are lost per week in airports, job sites, in transit, and even within the employees own office
- Less than 4 percent of lost laptops are eventually recovered

What do we do?

- Full disk encryption on all portable computers, the laptop is left useless without the right un-encryption key
- Good asset management, all devices need to be accounted for through their lifecycle of purchase, use, and retirement
- Lo-Jack type devices are available, but the cost may be prohibitive for some organizations

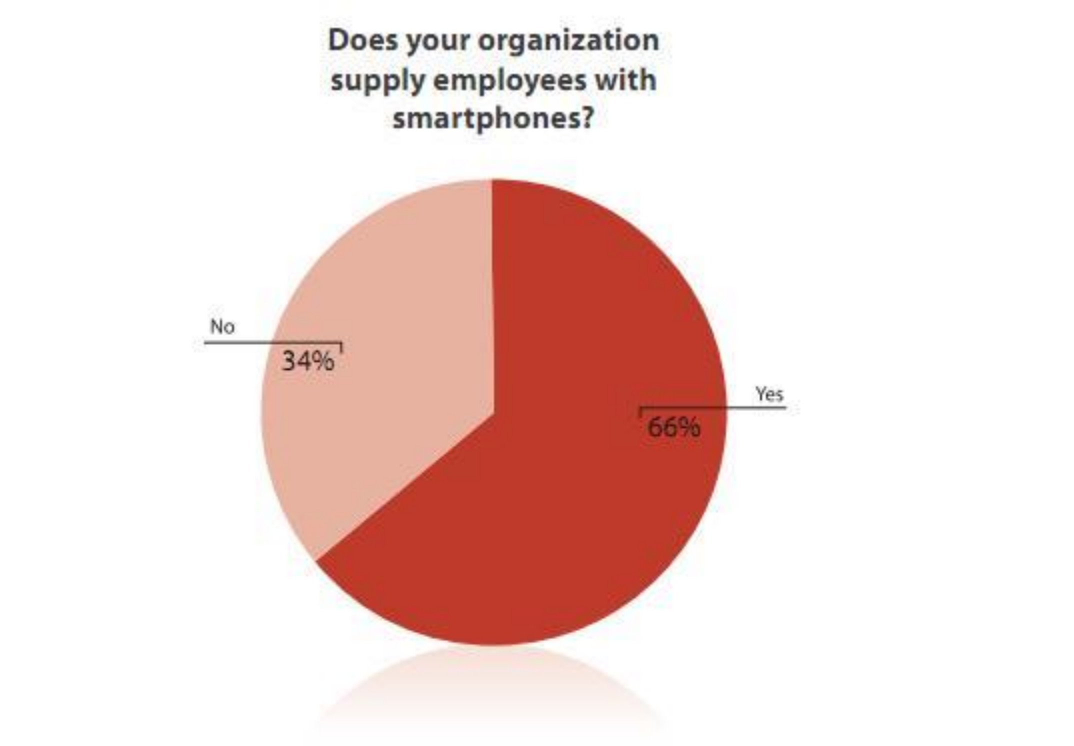
Remote Connectivity



Mobile Phones and Tablets

- Explosion of ownership over the past few years. 90% of U.S. adults own a cell or smart phone
- Multiple vendors and software flavors deployed making a single secure solution less viable
- Organizations may choose to provide phones or allow access from privately owned devices

Cellphones & Tablets



Does your organization supply employees with smartphones?

So where do the biggest risks lie?

- All of the security issues in latops existing in mobile
- On top of that Smartphones/Cellphones present different risk factors that traditional PC’s in that…
  - Devices are always on
  - Multiple connection pathways (cellular, Wi-Fi, Bluetooth)
  - Lost/Stolen/Misplaced in high numbers
  - Security measures are often not as robust

So where do the biggest risks lie?

- Though the sheer number of iPhones worldwide make them a particularly attractive target
- iPhones requirement to sync to iTunes has been listed as a possible vulnerability
- Increasing number of location tracking apps is also a concern as users may not know how to opt out

So what does this mean for business?

- Individuals are at risk for hacking/phishing/bluejacking and or loss of data for
  - Corporate network access
  - Company email
  - Contact lists
  - Sensitive data

So what does this mean for individuals?

- Individuals are at risk for fraud through hacking/phishing/bluejacking and or loss of data for
  - Family photos
  - Banking information
  - Personal email
  - GPS tracking info
  - Embarrassing photos

Mobile devices and the law

- Because of the blurring of "on-the-clock" and "off-the clock" time in modern business, both business and personal mobile devices could be seized as evidence in a lawsuit
- Bear in mind that the location of an employee (fraudulent or legitimate) could be admissible in court if you are sued
- Additionally, an employee’s Google/Yahoo searches (fraudulent or legitimate) could also be admissible in court in case of a lawsuit

Policy should include cont.

- Incident response guidelines that cover what will be reported, to who, procedures, hotline, etc.
- Security practices (software and hardware) that will be observed and monitored
- Define that mobile devices in the workplace have remote wipe capability
- Disposal, donation, destruction of devices (and their data) as the whole life cycle should be addressed

What do we do?

- Encryption, encryption, encryption
- Privacy guidelines that define what is and isn’t private when working on mobile devices (beware of applicable laws and regulations)
- Password guidelines that define the complexity, change frequency, and enforcement
- Storage and retention guidelines to address what will be kept, where, how long, etc.

What do we do?

- Treat all mobile devices, personal and business, as potential vulnerabilities
- Failure to address both (personal and business) under a common integrated security policy creates holes in your security
- Create and publish an “acceptable use” policy for all mobile devices brought into the workplace

What are companies doing today?

- Recently 1,400 IT professionals in 14 nations were asked what mobile device anti-fraud policies they have in place
- 21% had no restrictions
- 58% had "lightweight" policies such as banned apps or websites
- Only 20% had "stringent" guidelines

Questions???

Jay M Demmler

jdemmler@smu.edu