FERPA: Data & Transport Security Best Practices

Mike Tassey
Privacy Technical Assistance Center

April 2013
FERPA and Data Security

• Unlike HIPAA and other similar federal regulations, FERPA does not require specific security controls

• This provides room for innovation, but also heaps more responsibility on the community to protect the privacy and security of student data

• As educators we have student data in many places, including our own machines / mobile devices

• It’s up to us to ensure that we take the necessary security measures to protect student data
FERPA and Data Security

When we talk about data security we are really talking about these three things:

- **Confidentiality** — “Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec 3542]

- **Integrity** — “Guarding against improper information modification or destruction, and includes information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542]

- **Availability** — “Ensuring timely access to and use of information…” [44 U.S.C., Sec 3542]
FERPA and Data Security

- Data security is about risk management
- For there to be risk there must be vulnerability and someone to exploit it
- You can never eliminate risk, you can only reduce it
- To understand the risks, you must understand the threats
Let’s Talk About Threats

Organized Crime

• Criminal hackers and scammers
• Internet crime brings in big money, prompting leniency from local authorities in some countries
• Traditional organized crime has taken an interest
• Hundreds of billions a year
• Responsible for most external data breaches
• Botnets, malware, data breaches
Hacktivism (a portmanteau of hack and activism) is the use of computers and computer networks as a means of protest to promote political ends.

- Groups of hackers motivated by ideology or political agenda
- Largely decentralized, ad hoc organizational structure
- Historically focus on industrial, financial and political targets
- Increasingly targeting educational agencies

Let’s Talk About Threats

Nation-State Sponsored

- Cyber-espionage, cyber-warfare by foreign governments
- Spying, stealing intellectual property
- Intelligence gathering
- Prepositioning cyber-warfare assets
- Highly advanced, very sophisticated
- Virtually unlimited budget
- Stealth and longevity are priorities
Let’s Talk About Threats

The enemy is US!

- Lost laptops, smartphones, thumb drives
- Design insecure or flawed web applications
- Open attachments from strange people / fall for phishing emails
- Send information we shouldn’t
- Misconfigure our devices
- Use untrusted Wi-Fi for sensitive activities
What do the bad guys want with my data?

- Identity information like SSNs, banking info, names and other PII
- Prove a point, make a statement
- Account info (usernames & passwords)
- Recruit your system as a part of a Botnet
More dangerous than ever

- Open source and free tools make it easy
- Hacker training sites
- Cyber-theft commoditized
  - Black market trading in identity data
  - “Do-It-Yourself” malware kits
  - Underground economy where tools are built and sold to order
- Still developing flawed code
  - Structured Query Language Injection (SQLi) discovered in 1998.. Still a major problem 15 years later
  - Poor authentication / session mgmt.
Security begins with strategy

- Starts with leadership buy-in
- Create a strong information security policy & governance architecture that is reflective of reality
- Dedicate resources to security, put someone in charge
- Implement tools, technology and automation
- Develop meaningful metrics to measure the effectiveness of your program
“Defense in Depth”

- Use a layered approach to security which forces attackers to traverse multiple layers of security controls like firewalls, Web Application Firewalls (WAFs), Intrusion Detection / Prevention Systems (IDPS), antivirus, access controls, etc.

- Increases attacker effort

- Multiplies the opportunity for detection and response

- Allows you to focus the highest levels of resources where they count the most… protecting the really important data!
Data Security best practices

Patch & Vulnerability Management

- Employ tools to manage system updates and patches and remediate unpatched systems
- Especially important for third party applications
- Scan regularly for vulnerabilities and stratify validated results into a remediation plan that is ordered by severity
- Develop a procedure for deployment of updates and patches that is in line with your security policy, measure the results
- Tie results into security testing activities
Data Security best practices

Account / Password Management

- Require strong, complex passwords which are changed regularly
- Balance requirements against user acceptance. Users find ways to get around unreasonable security measures
- Consider multi-factor authentication for sensitive accounts
- Carefully monitor and manage user and service accounts to remove old or unused accounts and properly on-board new users
Data Security best practices

Encryption

- Encryption is not a replacement for good access control mechanisms
- Can be used to prevent accidental disclosure though loss of hardware like a laptop, mobile device or USB thumb drive
- Choose commonly accepted strong algorithms like those found in the Federal Information Processing Standard (FIPS) 140-2
- Key management can be challenging and the impact of lost keys can be high
What is Data Transport

- The movement of data from one system to another, often referring to the movement of large datasets to a data warehouse or the sharing of data between data systems.
- Transport mechanisms can include a variety of protocols and technology.
- Diversity of solutions can reduce efficiency of data transfer and increase attack surface.
- Some methods can introduce security vulnerabilities and lead to potential disclosure of data.
Data Transport security best practices

It’s all in the protocol

• When using removable storage or email, consider encryption to protect the data from loss or theft in transit

• Some transport mechanisms like File Transfer Protocol (FTP) provide little to no protection for authentication credentials or the data in transit

• Combining technologies has closed some of the security gaps:
  • FTPS or FTP Secure combines FTP with Transport Layer Security (TLS) / Secure Sockets Layer (SSL) to encrypt data in transit
  • SFTP combines the functionality FTP with the encryption capabilities of the Secure Shell (SSH) to provide a layer of encryption for transport
Data Transport security best practices

- Web services based transport mechanisms allow for a wide variety of functionality, allowing a single web service to serve as a hub for multiple applications.
- Several standards exist today for the creation of web services driven data transport mechanisms for education systems.
- Test the security of all data transport systems periodically and as needed to evaluate the security posture of the organization.
The price is high.
Protecting ourselves

• Understand the threat

• Know yourself and your vulnerabilities
  • Identify the “Crown Jewels” and protect them first
  • Assess your own systems, view them like an attacker

• Standardize (technology, data, procedures)
  • Adopt common methodologies and data standards
  • Band together with partners & share threat data

• Don’t rely on technology alone to keep you safe
  • Train users to be aware and exercise safe browsing habits
  • Be ready to respond to incidents quickly and efficiently
Protecting ourselves

- Mitigate the threat where you can
  - Make what you already have work better
  - People are the key, awareness is a powerful weapon

- Monitor & Manage your data
  - Collect logs that make sense
  - Retain information to help reconstruct events which may have occurred in the past

- Be ready to respond
  - Have a response plan
  - Identify response team in advance and set aside the resources needed
  - Periodically test response capability with simulated events
ED/PTAC Resources available

- Case Studies
  - H.S. Feedback Report
  - Head Start Program
  - FPCO Enforcement of FERPA
  - PTAC Technical Assistance

- Data Sharing
  - Data Sharing Agreement Checklist
  - Guidance for Reasonable Methods

- Data Security
  - Data Security Checklist
  - Data Governance Checklist
  - Cloud Computing
  - Identity Authentication Best Practices
  - Data Breach Response Checklist
Additional ED/PTAC Resources:

- Disclosure Avoidance FAQs
- Identification of Data Types & Uses
- De-identified Data Case Study
- FERPA 101 professional training video
- FERPA 201 (Data Sharing) professional training video
- FERPA 301 (Postsecondary) professional training video
Contact Information

Family Policy Compliance Office
Telephone: (202) 260-3887
Email: FERPA@ed.gov
FAX: (202) 260-9001
Website: www.ed.gov/fpc0

Privacy Technical Assistance Center
Telephone: (855) 249-3072
Email: privacyTA@ed.gov
FAX: (855) 249-3073
Website: www.ptac.ed.gov