Cyber Security

Companies, governments, and consumers depend on secure and reliable computer networks and data products. But as technology becomes more complex, security threats also become more complicated. Wireless networking, proprietary digital media, and the world-wide proliferation of high-speed computers all introduce new cyber-security challenges. Cyber-security researchers at the University of Maryland are developing the technologies and security strategies that will enable secure data transmission and storage on the systems of today and the networks of the future. Maryland researchers have expertise in wireless network security, security monitoring, cryptography, multimedia forensics, secure programming, and the economics of security threats.

William Arbaugh leads the Maryland Information Systems Security Lab. He designs dynamic security auditing systems that use historical data to predict and preempt new attacks. Arbaugh also investigates and develops wireless networking standards.

Jonathan Katz develops and improves sophisticated mathematical and biometric cryptography for secure networking. These algorithms can help secure large, open infrastructures, such as corporate and university networks.

Min Wu's forensic encryption algorithms can help track the circulation of large files, such as video files and satellite photos. Her image "fingerprint" technologies can help combat media piracy and protect sensitive files, like military intelligence images.

Jeffrey Hollingsworth creates tools to help programmers detect security flaws early in the software development cycle. He also creates secure authentication protocols for vulnerable distributed networks.

Lawrence Gordon and Martin Loeb examine the economics of information security. The Gordon-Loeb Model for information security investment provides businesses with a framework for determining how much they should spend on securing their information assets.

Secure Co-pilots for Preventing Network Attacks

William Arbaugh, head of the Maryland Information Systems Security Lab (MISSL), oversees projects ranging from wireless networking security to trustworthy computing and traditional operating systems security. One of Arbaugh's projects is the development of secure "co-pilot" systems: independent auditing platforms that can detect and respond to security violations. These auditors are hard-wired into independent embedded processors, which allows them to react to problems even if a network host is compromised. Programmed with sophisticated event-recognition policies, these prescient "oracles" can predict the onset of an attack based on triggering events in network traffic. Thus, a co-pilot system can respond at the initial signs of an attack before a virus or worm can compromise critical components.

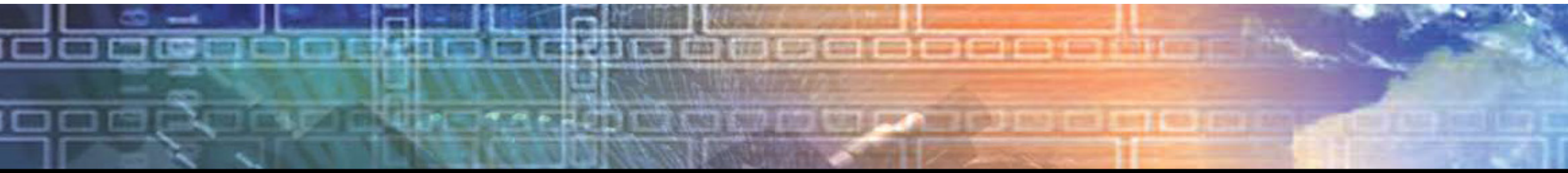
Arbaugh has also developed ways to review historical incident data to learn from past mistakes and improve security management. For example, this data analysis can improve the policies that his co-pilots use for detecting and reacting to threats.

In his research on wireless networks, Arbaugh has discovered problems in existing cryptographic systems for the 802.11 standard, the wireless standard used by consumers and businesses throughout the world. Arbaugh's work will make the next generation of wireless networks more secure.

William Arbaugh warbaugh@umd.edu http://www.cs.umd.edu/~waa/

Exposure-Resistant Keys for Cryptographic Systems

Jonathan Katz is an expert in the mathematical analysis of security problems and in designing and analyzing cryptographic protocols and tools. One of Katz's research interests is the development of exposure-resistant secret keys. Secret keys are information parameters used by cryptographic algorithms to decipher encrypted information passed between authenticated parties.



The exposure of secret keys can be a devastating attack, since such an attack typically means that all security guarantees are lost. The threat of key exposure is becoming more acute as cryptographic algorithms are increasingly deployed on small, mobile, and easily compromised devices. Katz models different ways to protect against key exposure, and designs resilient provably-secure systems. One of Katz's innovations has been to develop an encryption scheme whose secret keys evolve over time. Even if a key is exposed, an intruder would not be able to permanently break the cryptographic system.

Katz also developed the first provably-secure system for identity-based encryption. Such a system could be used in large, open institutions such as universities to generate encryption keys for employees and students.

Jonathan Katz jkatz@cs.umd.edu http://www.cs.umd.edu/~jkatz

Securing Digital Media

Min Wu develops more secure ways to transmit data, particularly multimedia files such as digital images and videos. Wu works to ensure that authentic information is delivered and used only by authorized users for authorized purposes. Her digital fingerprinting technology embeds invisible identifiers within an image whenever the file is used, altered, or transmitted. The authority that created the rules generating the identifiers can then track the circulation and integrity of an image based on these markers.

Her research, with its ability to trace leaks, offers important capabilities for the intelligence community. It can also be used to discourage media piracy by protecting the proprietary material of the movie industry. Wu's work is funded by the Department of Defense and the National Science Foundation.

Min Wu minwu@eng.umd.edu http://www.ece.umd.edu/~minwu

Dynamic Code Analysis

Jeffrey Hollingsworth works on code analysis and code development. He creates interfaces, tools, and analytic programs that allow programmers to write code that minimizes security flaws. The work aims to provide developers with instant feedback that audits code for potential threats as they write it, so security vulnerabilities are identified early in the development process.

Hollingsworth is an expert in dynamic code analysis. Rather than examining the source code itself, this kind of analysis examines the behavior of software and infers security bugs based on changes in this behavior.

For future software, Hollingsworth is helping develop new computing languages that encourage secure programming at the most basic level. Hollingsworth also develops software architecture that improves the security and performance of distributed computing. He and his coworkers are designing a multi-level security scheme that automatically adjusts data and code according to the degree of trust established between systems.

Jeffrey Hollingsworth hollings@umd.edu http://www.cs.umd.edu/users/hollings/

Enabling the Cost-Benefit Analysis of Information Security

While some organizations have near infinite security resources, business executives must often make security decisions based on cost. Lawrence Gordon and Martin Loeb, economists with the university's Robert H. Smith School of Business, develop quantitative methods that can inform these decisions.

The Gordon-Loeb Model for information security characterizes the optimal level of investment for protecting an information asset. Gordon and Loeb's model has shown that it is generally uneconomical to invest in a security strategy more than 37 percent of the expected loss that would occur from a security breach. The Gordon-Loeb Model also shows that the optimal amount to spend protecting an information asset does not always increase with increases in the asset's vulnerability.

Lawrence Gordon	lgordon@rhsmith.umd.edu	http://www.rhsmith.umd.edu/accounting/faculty/gordon.html
Martin Loeb	mloeb@rhsmith.umd.edu	http://www.rhsmith.umd.edu/faculty/mloeb/