Aleksandr Yampolskiy

Director of Security and Compliance at Gilt Groupe

yampolskiy@gmail.com

Specialties

Architecture of highly available, distributed, fault-tolerant solutions, Cryptography, Authentication, Presented at Numerous International Conferences.

Experience

Director of Security and Compliance at Gilt Groupe
October 2009 - Present (1 year 3 months)

Head of Security & Compliance team.

• Created Security and Compliance team with responsibilities for risk management, compliance, fraud investigations, secure coding, IT and infrastructure security, and security awareness and training.
• No vulnerabilities exploited since the team was established.
• Established channels for internal escalation of security events (through various security-* mailing lists, JIRA security categories, etc.)
• Developed an incident response policy and SLAs for fixing critical bugs. For example, a recent critical Adobe patch was remediated on the same day.
• Produced regular program reports, risk metrics and compliance status for Gilt's executive and non-executive management.
• Automated many security processes and reporting to become a more efficient organization.
• Oversaw PCI DSS compliance efforts to ensure all cards are stored in a very secure, PCI compliant environment.
• Managed development and implementation of global information security policies and procedures (aligned to ISO 27002) from scratch.
• Fraud mitigation efforts.

Please join Gilt for luxury brands at affordable prices: http://www.gilt.com/invite/ayampolskiy

Sr. Security Engineer at Goldman Sachs
October 2007 - October 2009 (2 years 1 month)

Subject matter expert in authentication/entitlements/cryptography.

• Served in various working groups to help establish firmwide policies on JMX security, cryptography, Sharepoint authentication, and secure credential management.
• Advised various business units on best practices for integrating authentication/entitlements into

their products, while complying with internal/external policies and regulations
• As a Local Security Coordinator, I helped developers to timely remediate software vulnerabilities.
• Re-architected in-house IDM system to track system ID accounts (Java, Perl, SQL stored procedures) whose passwords do not expire. This established better internal controls for SOX compliance.
• Developing Permit (next-generation entitlement system) (Java).
• Lead development of the Blackberry single-sign on authentication server, which authenticates Blackberry handheld devices (Java, SQL)
• Serve as a firmwide expert on authentication and cryptography issues. As part of that, traveled to China to build their authentication infrastructure.
• Developed a .NET GSAuthNClient library which allows clients to perform authentication operations against back-end WebID authentication service .
• Developed ICORN IIS plugin which supports new authentication tokens (C/C++, ISAPI filter) and security constraints.
2 recommendations available upon request

Sr. Member of Technical Staff at Oracle Corporation
June 2006 - October 2007 (1 year 5 months)

Responsible for developing identity management and security software, focusing on security, authentication and federated identity protocols (e.g., SAML, Liberty Alliance and WS-Security).

• Added support in the Oracle Identity Federation server for X509 attribute mapping/filtering (Java).
• Implemented JMX MBeans to remotely provision users/roles in the LDAP data store used by Oracle's JAZN (authorization/policy provider) (Java).
• Improved performance of Oracle crypto toolkits and made them compliant with Sun JCE standards (Java, C++).
• Developed a QA suite of JUnit and regression tests for ASCTL (a scripting language used to configure Oracle Application Server) (Java, Jython).
1 recommendation available upon request

Researcher at Yale University
September 2001 - May 2006 (4 years 9 months)
• Analyzed various security problems from combined economic and cryptographic points of view.
• Designed a mechanism to spread signals furtively across the network.
• Proposed a game-theoretic model for containment of viruses in a network.
• Invented a way of protecting documents from a malicious storage provider by entangling them together.

Volunteer Administrator at chessclub.com
September 1999 - May 2006 (6 years 9 months)
* Provide advice on technical aspects such as server design, security, etc.
* Liaison with Russian speaking chess players.

Software Design Engineer (Intern) at Microsoft Corporation
June 2003 - August 2003 (3 months)

Responsible for backup functionality in Windows Live OneCare safety scanner:
• Implemented a COM module for disaster recovery from backup CDs (C++).
• Developed an AUTORUN application that launches when a user inserts a backup CD into the computer (C/C++).
• Interacted with other developers, program managers, and the client UI team to integrate AUTORUN component with the rest of the product (C#).
• Created a UI for the disaster recovery module, which displays a list of backed up files in a tree-like structure (C#).
2 recommendations available upon request

Researcher at Distributed and Parallel Systems Group
July 2000 - September 2000 (3 months)

- Investigated migration of process states across arbitrary networks.
- Developed API to intercept Win32 function calls using MS Detours library (C).
- Implemented a fault-tolerant replicated state machine simulator (Java, Perl).

Education

Yale University
M.S., M.Phil., Ph.D., Cryptography, 2001 - 2006
Activities and Societies: Second board in Yale chess team.
President of Yale Russian club YANIS, 2005-2006.

New York University
B.A., Mathematics, Computer Science, 1997 - 2001
Activities and Societies: Phi Beta Kappa, Dean's Honors List, Summa Cum Laude

Sinai Academy

Honors and Awards

Best Paper Award in Public Key Cryptography (PKC 2006) conference out of 126 submissions

Interests

entrepreneurship, business networking, cryptography, chess, travel, acting, martial arts

Aleksandr Yampolskiy

Director of Security and Compliance at Gilt Groupe

yampolskiy@gmail.com

Linked in

5 people have recommended Aleksandr

"Alex is congenial to work with, passionate about security and cryptography and good at time management. He has always displayed insights by brainstorming security issues during code and design reviews. I would place him on par with one of the best senior members to have worked with."

— **Anil S B***, Sr. Security Engineer, Security Engineering Team, Goldman Sachs*, worked indirectly for Aleksandr at Goldman Sachs

"Aleksandr is a very capable computer security expert. He has a wealth of knowledge in the field and knows how apply it. His scientific research, educational and professional background allows him to solve the most complicated problems quickly and in a non trivial but elegant way. He is a capable developer versed in wide array of technologies. He has great leadership and organizational skills that allow him to be a natural leader in the company of his peers. His opinions matter and are well listened to by upper management. Aleksandr would be a great addition to any team as he makes invaluable contribution to any project he is involved in."

— **Denis Kezerashvili***, Java Architect, Goldman Sachs*, worked directly with Aleksandr at Goldman Sachs

"I met Alex when we both interned as Software Developers at Microsoft in 2003 and we have remained friends since then. When I was employed full-time at Microsoft, Alex was formally offered a summer Research Intern position with Microsoft Research, an honorable position, but chose to focus on finishing his Yale PhD in cryptography. Alex immediately struck me as an exceptionally bright fellow. He is a passionate critical thinker with leadership qualities, an ability to take on responsibility, matching social skills, and an insatiable desire for self-improvement."

— **Leonid Velikovich***, Software Design Engineer Intern, Microsoft*, worked with Aleksandr at Microsoft Corporation

"Alex was a key stakeholder in the Identity Federation product team at Oracle, where his superb technical knowledge and development talent helped drive this product forward successfully, and demonstrated a keen sense to priorities, flexibility and focus on results that proved critical as the product release schedule and technical challenges weren't trivial to deal with. Alex knowledged of the security and identity management technical areas is impressive, and he has proven that he can

successfully apply it to achieve measurable results."

— Frank Villavicencio, *Director of Product Management, Oracle Corporation*, managed Aleksandr indirectly at Oracle Corporation

"Alex was a smart, easy going, and hard working colleague. I worked with him when working towards PhD at Yale University. I believe everybody will enjoy working with him just like me."

— Sheng Zhong, *Student, Yale University*, worked with Aleksandr at Microsoft Corporation

Contact Aleksandr on LinkedIn