### I. Title of Request (please be brief):

Department Number/Department Name: 360 College of Computing

Virtualized Infrastructure for Information Security

**Amount of Request (formula from detailed budget below):** $60,665

Yes No

Yes

### Executive Summary of Request (100 words or less):

We propose to purchase the necessary equipment to modernize the Information Security and Network Security courses, providing virtual machines that can be exposed to security risks, without endangering the campus and College of Computing networks.

### Specific class and/or lab initiative(s) if applicable:

David Mercer (5-2518), Manos Antonakakis

Contact person for this request (incl. phone #):

Indicate priority per department if applicable:

Number of

Number 2 of 10

### II. Impact on Students - Provide course title, course number, and anticipated enrollments:

<table>
<thead>
<tr>
<th>Titles/Numbers of Course(s)</th>
<th>Anticipated Enrollments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS4035/6035, CS6262/ECE8813, CS6265</td>
<td>Graduate: 1,000 per sem per year</td>
</tr>
<tr>
<td></td>
<td>Undergraduate: 250 per sem per year</td>
</tr>
<tr>
<td></td>
<td>Total: 1,250 per sem per year</td>
</tr>
</tbody>
</table>

**NOTE:** Other impacts on students should be described in narrative.

The new Institute for Information Security & Privacy (IISP) has recently launched several new educational programs to meet the growing nationwide demand for cybersecurity professionals. Accordingly, the MS degree program in Information Security (MS-INFS) and information security courses that are offered to undergraduate and graduate students in the College of Computing have started to draw considerable attention from a larger audience; in particular, information security hosted programs sponsored by industry and government in CS6262/ECE8813, and undergraduate students in CS4235. We expect that over 1000 students each year will take an information security course that includes a project component requiring access to a secure and isolated instructional laboratory. Our current information security laboratory has limited capacity and its facilities are outdated. In a recent appraisal by the Academic Program Review (APR) external committee, constituted by the Provost’s office for the MS-INFS program, pointed out in its report that our current infrastructure to support security classes is outdated and inadequate in terms of quality and quantity for meeting program instructional needs. In this proposal, we describe our plan for modernizing the current infrastructure and how to effectively utilize the new infrastructure for multiple courses that will benefit thousands of students in the future.

### III. Narrative - Provide narrative justification for your intended use of the technology fee funds. Include narrative on how the education or research of the students will be enhanced. Also include how the request aligns with the Strategic Plan of Georgia Tech. Continue in the block below if necessary.

The new Institute for Information Security & Privacy (IISP) has recently launched several new educational programs to meet the growing nationwide demand for cybersecurity professionals. Accordingly, the MS degree program in Information Security (MS-INFS) and information security courses that are offered to undergraduate and graduate students in the College of Computing have started to draw considerable attention from a larger audience; in particular, information security hosted programs sponsored by industry and government in CS6262/ECE8813, and undergraduate students in CS4235. We expect that over 1000 students each year will take an information security course that includes a project component requiring access to a secure and isolated instructional laboratory. Our current information security laboratory has limited capacity and its facilities are outdated. In a recent appraisal by the Academic Program Review (APR) external committee, constituted by the Provost’s office for the MS-INFS program, pointed out in its report that our current infrastructure to support security classes is outdated and inadequate in terms of quality and quantity for meeting program instructional needs. In this proposal, we describe our plan for modernizing the current infrastructure and how to effectively utilize the new infrastructure for multiple courses that will benefit thousands of students in the future.

### IV. Detailed Budget - Requested Items by Category

List separately any equipment, software, and other allowable expenses (see Tech Fee Guidelines). There is a formula in the "total column" that multiplies the number of items times the unit price. You may enter a figure into the total column if the unit pricing is not applicable. If you need additional rows, contact the Budget Office to receive a modified form.

**Supporting documentation is required** - Include price justification in some form, such as quotations, published price lists, etc. as a separate PDF attachment. All supporting information should be in a single PDF.

<table>
<thead>
<tr>
<th>Proposed Number of Items</th>
<th>Estimated Price per Unit</th>
<th>Total ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Compute Nodes</td>
<td>6</td>
<td>$7,475</td>
</tr>
<tr>
<td>VM Storage Node</td>
<td>1</td>
<td>$7,575</td>
</tr>
<tr>
<td>IDA Pro Software Package</td>
<td>1</td>
<td>$8,140</td>
</tr>
<tr>
<td>Cables</td>
<td>1</td>
<td>$100</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Please return form via e-mail in Excel format to: tina.clonts@business.gatech.edu. Supporting information only in a PDF file.**
III. Continuation of narrative justification, if necessary

The proposed technology fee funds will be used to expand the College’s existing virtualization infrastructure to bring three core information security courses to an expanded number of students. Taesoo Kim, Manos Antonakakis, and Wenke Lee will share the proposed infrastructure for labs and projects in Introduction to Information Security (CS4235/6035), Information Security Lab (CS6265), and Networking Security (CS6262/ECE8813). The key idea is to 1) provide an isolated, virtualized environment for safe cyber-security practices (e.g., pen-testing) and 2) share this infrastructure with other faculty at the IISP, as well as industry-sponsored students that will access the resource remotely.

Unlike typical needs for virtualizing computation resources (e.g., cost saving), virtualization in cyber-security education is critical in that students are dealing with potentially dangerous malware, developing attack payloads (i.e., exploits) against real-world software, and requiring unusual network typologies or outdated software stacks for security practices (e.g., pen-testing). Through this proposal, our team will be able to build and share a secure, suitable infrastructure to educate future information security professionals. We believe this proposal is not only the key to bringing our courses to a broader set of students, but also to deliver new types of security courses (e.g., capture-the-flag competition) which are not possible in our current infrastructure. Furthermore, as IISP is currently exploring multiple hosted offerings of the MS-INFS program, the proposed upgrades are critical for successful delivery of lab-oriented courses.

Each PI has a specific plan to utilize the proposed infrastructure.

Course CS6265, instructed by Taesoo Kim, currently has an enrollment of 30 master students with the potential to open up for senior undergraduates. Through 10-12 carefully designed labs in capture-the-flag competition style, students gain hands-on experiences in exploiting local/remote services, hacking on different architectures, pen-testing, fuzzing etc. The proposed infrastructure will be heavily used in this course to 1) provide safe, controlled and isolated workspaces for every student so they can practice hacking skills anytime anywhere and 2) provide fast and scalable emulation of various software stacks/hardware features so students can be up-to-date with the latest developments in the security industry.

Course CS6262/ECE8813, instructed by Manos Antonakakis, has a regular enrollment of 100 students. A critical component of this course is 1-2 lab sessions which train students on performing network packet auditing/analysis for intrusion detection and malware analysis. The proposed infrastructure will be used in this course to enable flexible configuration of network topology for these lab sessions, giving students, especially industry-sponsored students, the opportunity to work on real-world scenarios.

Course CS6035, instructed by Wenke Lee, has 100 on-campus students. A unique component of this course is 1-2 projects which train students with malware analysis. In particular, students will run real-world malware samples in isolated virtual machines, with special firewall policies and active monitoring. The proposed infrastructure will be used in this course to provide isolated and controlled virtual machines for students, instead of relying on them to install these tools on their own laptops. In addition, the proposed infrastructure will be used to emulate various operating systems (e.g., various Windows, including outdated ones) that would typically be unsafe to attain or deploy through other methods.