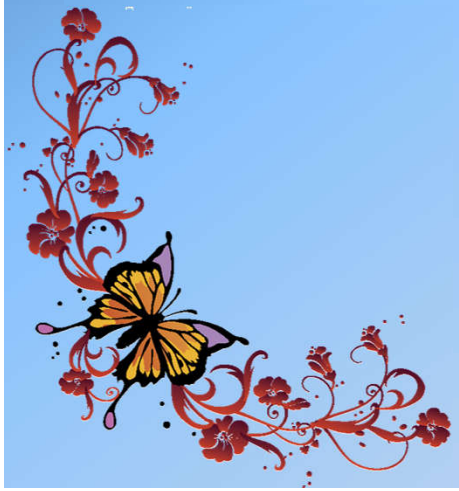
معرفی مرکز آپا دانشگاه صنعتی شریف



دانشکده‌ی مهندسی کامپیوتر
دانشگاه صنعتی شریف

آبان‌ماه ۱۳۹۵

سرخط

- مراکز آپا
- معرفی آپا دانشگاه صنعتی شریف
- فعالیت‌های انجام شده در مرکز آپاشریف

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

مراکز امداد و واکنش به رخدادها (CERT)

مراکز امداد و واکنش به رخدادها

- CERT → Computer Emergency Response Teams
- CSIRT → Computer Security Incident Response

نامی است برای گروه‌های تخصصی مدیریت رخدادهای امنیتی

مراکز امداد و واکنش به رخدادها

- تاریخچه گروه پاسخ‌گویی حوادث به پیدایش کرم‌های رایانه‌ای مرتبط می‌شود.
- کرم موریس در تاریخ ۳ نوامبر ۱۹۸۸ فعالیت اینترنت را مختل نمود.
- این حادثه منجر به شکل‌گیری اولین گروه پاسخ‌گویی حوادث در دانشگاه کارنگی ملون گشت که طی قراردادی با دولت ایالات متحده صورت پذیرفت.
- با توجه به رشد و گسترش سریع بهره‌گیری از فن‌آوری‌های اطلاعات و ارتباطات در سال‌های بعد، واژه‌ی جدید CERT و یا CSIRT به بخش و واحد لاینفکی از ساختار سازمان‌ها برای حفظ اطلاعات و کاهش رخدادهای امنیتی و جلوگیری از بروز تبعات بعدی، تبدیل گشت.

خدمات عمومی مراکز CERT

- خدمات واکنشی (Reactive)
- خدمات پیش‌دستانه (Proactive)
- خدمات مدیریت کیفیت امنیت

(Security Quality Management Services)

خدمات واکنشی (Reactive)

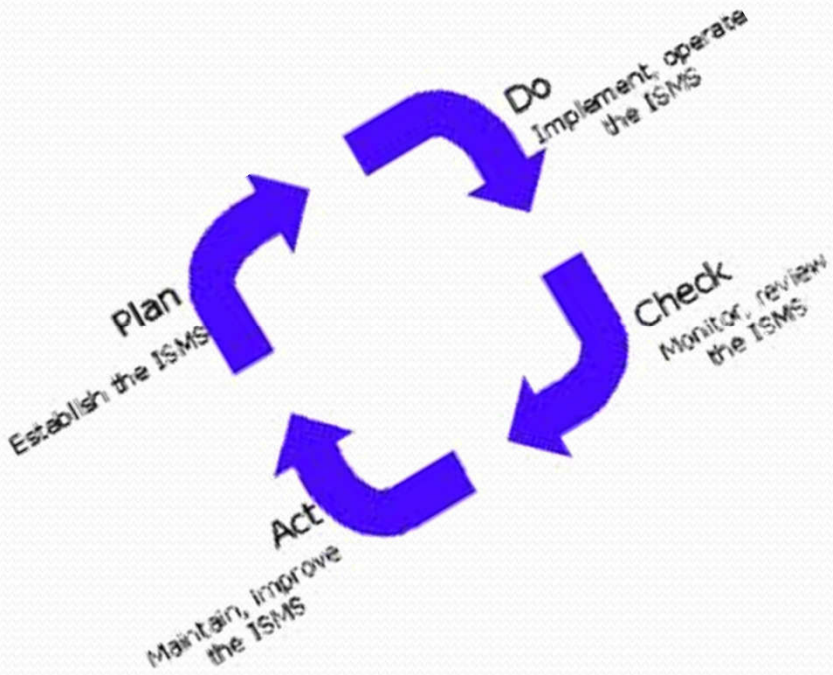
- اعلان اخطارها و هشدارها
- رسیدگی به رخداد
  - بررسی، پاسخ‌گویی و هماهنگی
- رسیدگی به آسیب‌پذیری‌ها
  - بررسی، پاسخ‌گویی و هماهنگی
- رسیدگی به بدافزارها و کدهای آسیب‌رسان
  - بررسی، پاسخ‌گویی و هماهنگی

خدمات پیش‌دستانه (Proactive)

- اطلاع‌رسانی و آگاهی‌رسانی
- ممیزی یا ارزیابی امنیتی
- توسعه ابزارهای امنیتی
- خدمات تشخیص نفوذ
- انتشار اطلاعات مرتبط با امنیت

خدمات مدیریت کیفیت امنیت

- برنامه‌ریزی تداوم کسب‌وکار و بازیابی از بحران
- مشاوره‌ی امنیتی
- آموزش
- ارزیابی یا صدور گواهی محصول



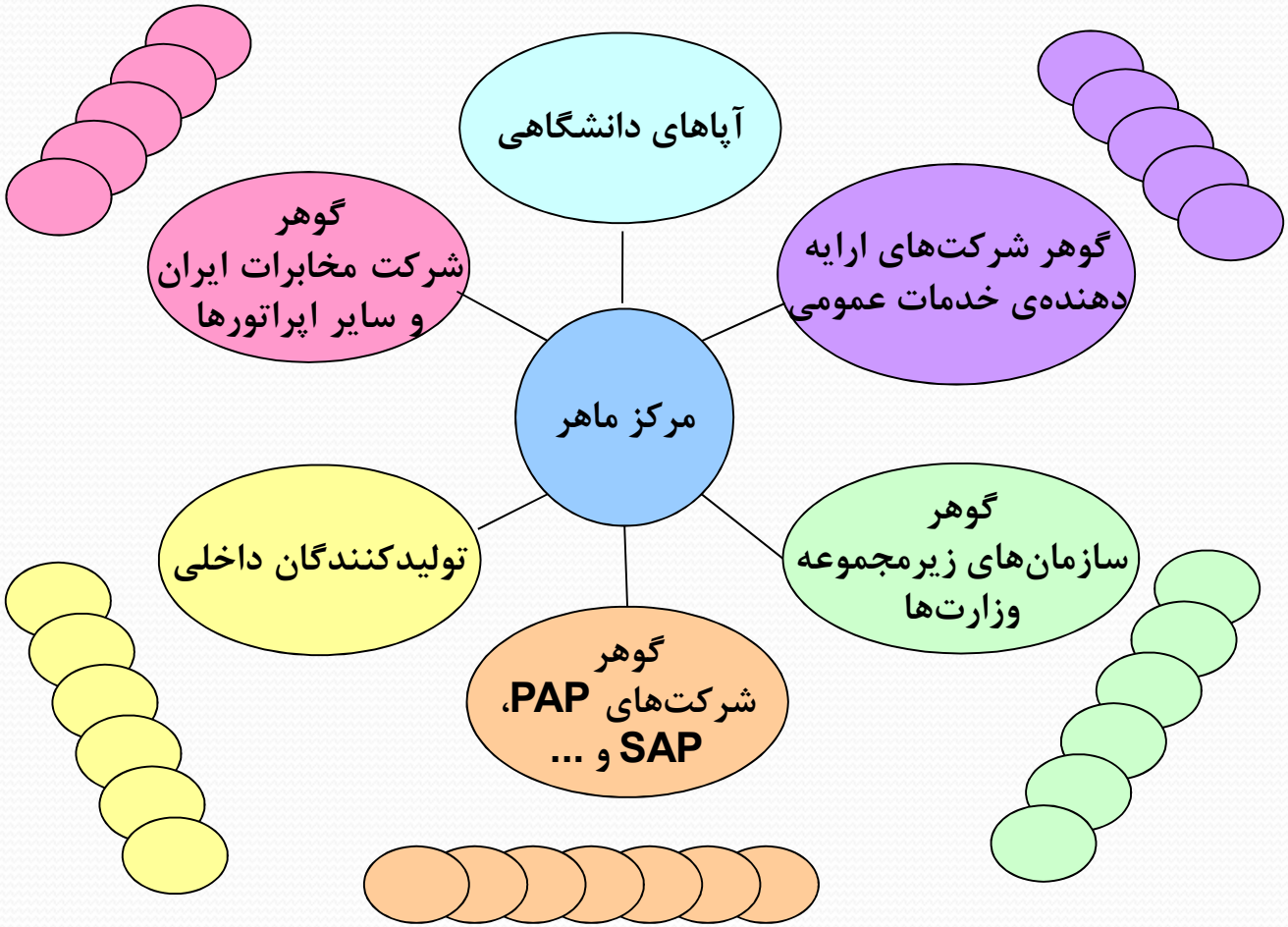
مراکز مدیریت رخداد در ایران

- **ماهر** مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای در سطح ملی و دولتی
- **گوهر** گروه واکنش هماهنگ رخداد سازمانی
- **آپا** مرکز آگاهی رسانی، پشتیبانی و امداد دانشگاهی
- **مهار** مرکز هماهنگی امداد رایانه‌ای نظامی

مرکز ماهر – اهداف

- ایجاد یک نقطه‌ی کانونی در سطح وزارت ارتباطات و فن‌آوری اطلاعات برای انجام فعالیت‌های هماهنگ راهبری رخدادهای فضای تبادل داده
- سیاست‌گذاری، توسعه و بهینه‌سازی روش‌های CSIRT
- بررسی امکانات بالقوه ایجاد امنیت در فضای تبادل داده‌ی کشور و کمک به بالفعل نمودن این امکانات
- کمک به تشکیل گروه‌های CSIRT در سازمان‌ها، شرکت‌ها و مراکز حوزه‌ی وزارت ارتباطات و فن‌آوری اطلاعات
- تسهیل ارتباط میان گروه‌های همسو و سازمان‌های مرتبط در راستای به اشتراک‌گذاری اطلاعات مرتبط با سلامت فضای تبادل داده
- توسعه مکانیزم‌های امن ارتباطی برای ارتباط مطمئن بین گروه‌ها
- عضویت در گروه‌های CSIRT آسیا و بین‌الملل و ایجاد تعاملات بین‌المللی

مراکز مدیریت رخداد در ایران

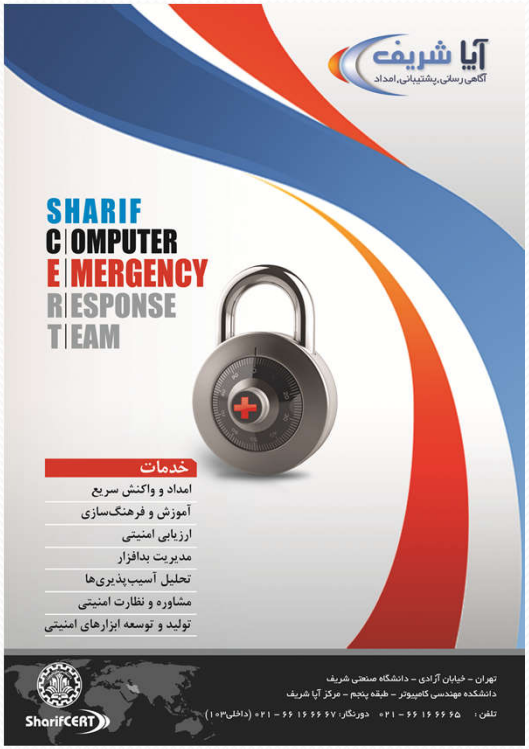


آپا شریف
آگاهی رسانی، پشتیبانی، امداد

مرکز آپا شریف

مرکز آپا شریف

- **آپا: آگاهی‌رسانی، پشتیبانی و امداد در حوزه افتا (CERT)**
- تاسیس در آذر ۱۳۸۶ در دانشکده‌ی مهندسی کامپیوتر دانشگاه صنعتی شریف
- با حمایت مالی و معنوی مرکز تحقیقات مخابرات ایران
  - در ابتدا ارائه خدمات آپا در حوزه‌ی پایگاه داده‌ها
  - آذر ۸۶ تا تیرماه ۸۸
- تغییر راهبرد پس از اتمام مرحله اول پروژه آپا
  - ارائه‌ی کلیه خدمات مراکز CERT
  - تحقیق، رصد، پیشگیری و مقابله با حوادث امنیتی



ماموریت آپا شریف

- آگاهی‌رسانی، آموزش و ارتقای دانش عمومی و تخصصی در زمینه‌ی امنیت، پیشگیری و مقابله با حوادث امنیتی در فتا
- ارائه‌ی خدمات فنی و تخصصی در زمینه‌ی اختلالات امنیتی مرتبط با فضای تبادل اطلاعات (فتا) از جمله پیشگیری و رسیدگی به حوادث، تحلیل و مدیریت آسیب‌پذیری‌ها و بدافزارها به منظور امن‌سازی فتا
- برقراری ارتباطات و همکاری‌های علمی و فنی ملی و بین‌المللی با مراکز امداد و واکنش رایانه‌ای داخل و خارج کشور در زمینه‌های مورد فعالیت مرکز
- ارتقاء جایگاه علمی دانشگاه صنعتی شریف از طریق پژوهش‌های فناورانه در حوزه‌ی امنیت فضای تبادل اطلاعات

عضویت در مجامع داخلی و بین‌المللی

- عضو عمومی CERT کشورهای اسلامی (OIC-CERT)

- عضو تعدادی از گروه‌های بین‌المللی مرتبط

- عضو مرکز هماهنگی آپاهای کشور (موسسه تحقیقات فاوا)

- عضو مرکز هماهنگی رخداد ماهر (سازمان فناوری اطلاعات ایران)

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

فعالیت‌های انجام شده در مرکز

فعالیت‌های مرکز آپا شریف

بیش‌تر فعالیت‌های مرکز آپا در سال‌های گذشته در قالب دسته‌های زیر بوده است.

- رصد و تحلیل حوادث رایانه‌ای
- آزمون نفوذ و ارزیابی امنیتی
- مشاوره در حوزه‌ی افتا
- آموزش در حوزه افتا
- توسعه و طراحی سامانه امنیتی (تشخیص و مقابله و ..)
- رقابت‌های نفوذ و دفاع در فضای مجازی

فعالیت‌های مرکز آپا شریف – رصد و تحلیل حوادث

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

- فاز اول و دوم پروژه‌ی آپا (در حوزه‌ی پایگاه‌داده‌ها)
  - بررسی آسیب‌پذیری‌های سمپادها
  - پیگیری اخبار و مقالات مرتبط با امنیت سمپادها
  - تهیه‌ی مستندات امن‌سازی

فعالیت‌های مرکز آپا شریف – رصد و تحلیل حوادث

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

- همکاری با مرکز ماهر در رصد و پایش حوادث و رخدادهای امنیتی
  - تحلیل بدافزارها
  - برگزاری دوره‌های آموزشی
  - مشارکت در پاسخ‌گویی به رخدادها
  - اطلاع‌رسانی و پیگیری حوادث

فعالیت‌های مرکز آپا شریف – رصد و تحلیل حوادث

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

- همکاری با مرکز ماهر در تحلیل بدافزارهای شبکه‌ی تله‌عسل
  - تحلیل و گزارش رفتار بدافزارهای جمع‌آوری‌شده
  - تهیه removal

فعالیت‌های مرکز آپا شریف – رصد و تحلیل حوادث

آپا شریف
آگاهی رسانی، پشتیبانی، امداد

- پاسخ‌گویی به رخدادها
  - شناسایی و پاک‌سازی ویروس stuxnet و گزارش‌های موردی
  - پاک‌سازی Duqu

فعالیت‌های مرکز آپا شریف – آزمون نفوذ و ارزیابی امنیتی

- آزمون نفوذ وب‌سایت‌ها و برنامه‌های کاربردی برای برخی سازمان‌ها
- ارزیابی امنیتی برنامه‌های کاربردی و زیرساخت شبکه

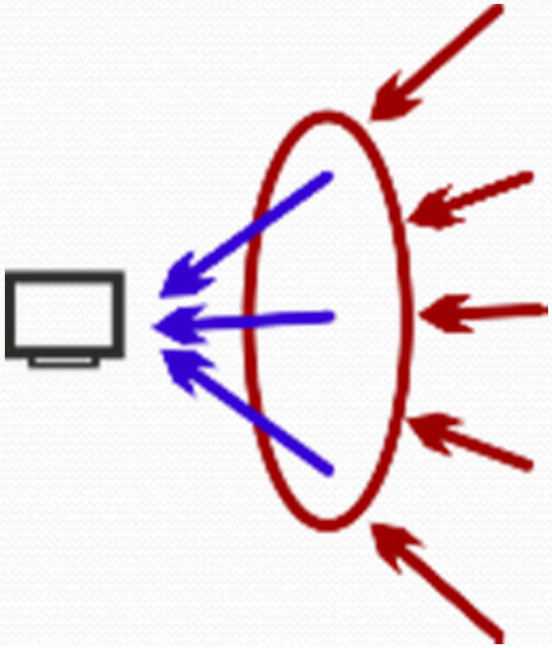
فعالیت‌های مرکز آپا شریف – مشاوره

- راه‌اندازی زیرساخت کلید عمومی، شناخت وضع موجود، امن‌سازی
- تامین امنیت سامانه‌ی جامع مالیاتی کشور (امنیت شبکه، نرم‌افزار، سیستم‌عامل‌ها و سرویس‌ها، پایگاه‌داده، زیرساخت‌های امنیتی مانند PKI، ساختار نیروی انسانی و تیم گوهر و ...)

فعالیت‌های مرکز آپا شریف –سامانه‌های تشخیص

- سامانه‌ی تابش (تلسکوپ آی‌پی شبکه)

کشف حملات مبتنی بر شبکه به کمک تحلیل ترافیک منتهی به فضای تاریک



- کشف حملات منع خدمت
- کشف گسترش کرم‌های امنیتی
- کشف پویش شبکه
- کشف پیکربندی نادرست شبکه

فعالیت‌های مرکز آپا شریف –سامانه‌های تشخیص

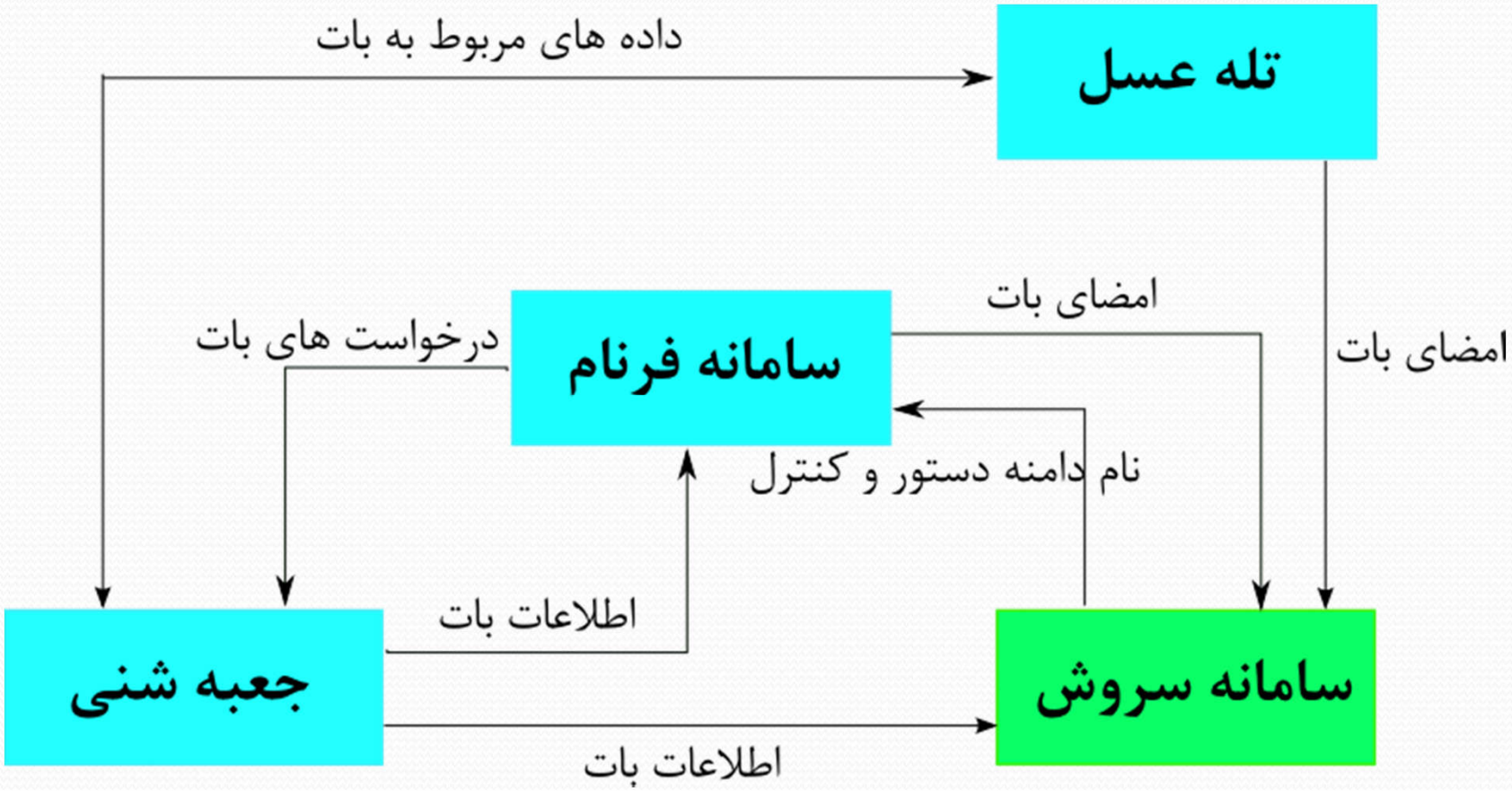
- سامانه‌ی سروش

- امروزه به دلیل گستردگی شبکه‌های بات و استفاده از فن‌آوری‌های متفاوت ارائه‌ی یک روش جامع برای کشف شبکه‌های بات کار دشواری است.

- سامانه‌ی سروش برای کشف شبکه‌های بات طراحی شده است.

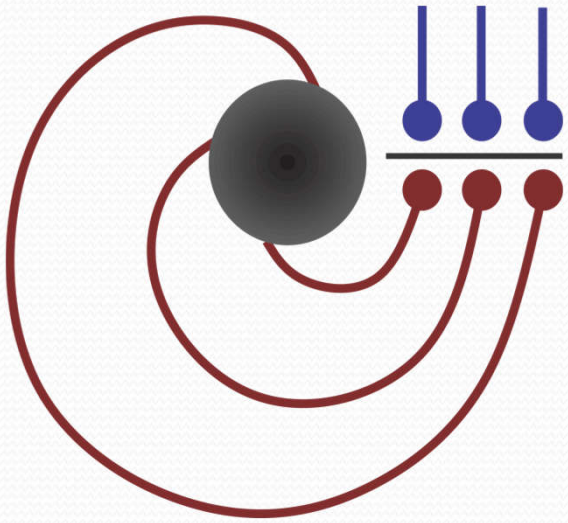
فعالیت‌های مرکز آپا شریف –سامانه‌های تشخیص

- سامانه‌ی سروش



فعالیت‌های مرکز آپا شریف –سامانه‌های تشخیص

- سامانه‌ی فرنام (فروچاله‌ی نام‌دامنه)
  - حملاتی که توسط شبکه‌های بات صورت می‌پذیرد، خسارت‌های جبران‌ناپذیری به سازمان‌ها وارد می‌کند.
  - یکی از روش‌های دفاعی در مقابل شبکه‌های بات استفاده از تکنیک فروچاله‌ی نام‌دامنه است.
  - مانع بات‌هایی می‌شود که از طریق سرویس DNS سعی در اتصال به کارگزار دستور و کنترل دارند.



فعالیت‌های مرکز آپا شریف – طراحی و توسعه‌ی سامانه

- تله‌عسل بومی (Honeypot)
  - طراحی و توسعه‌ی سامانه‌ی تله‌عسل بومی تلفیقی (کم‌تعامل و پرتعامل)

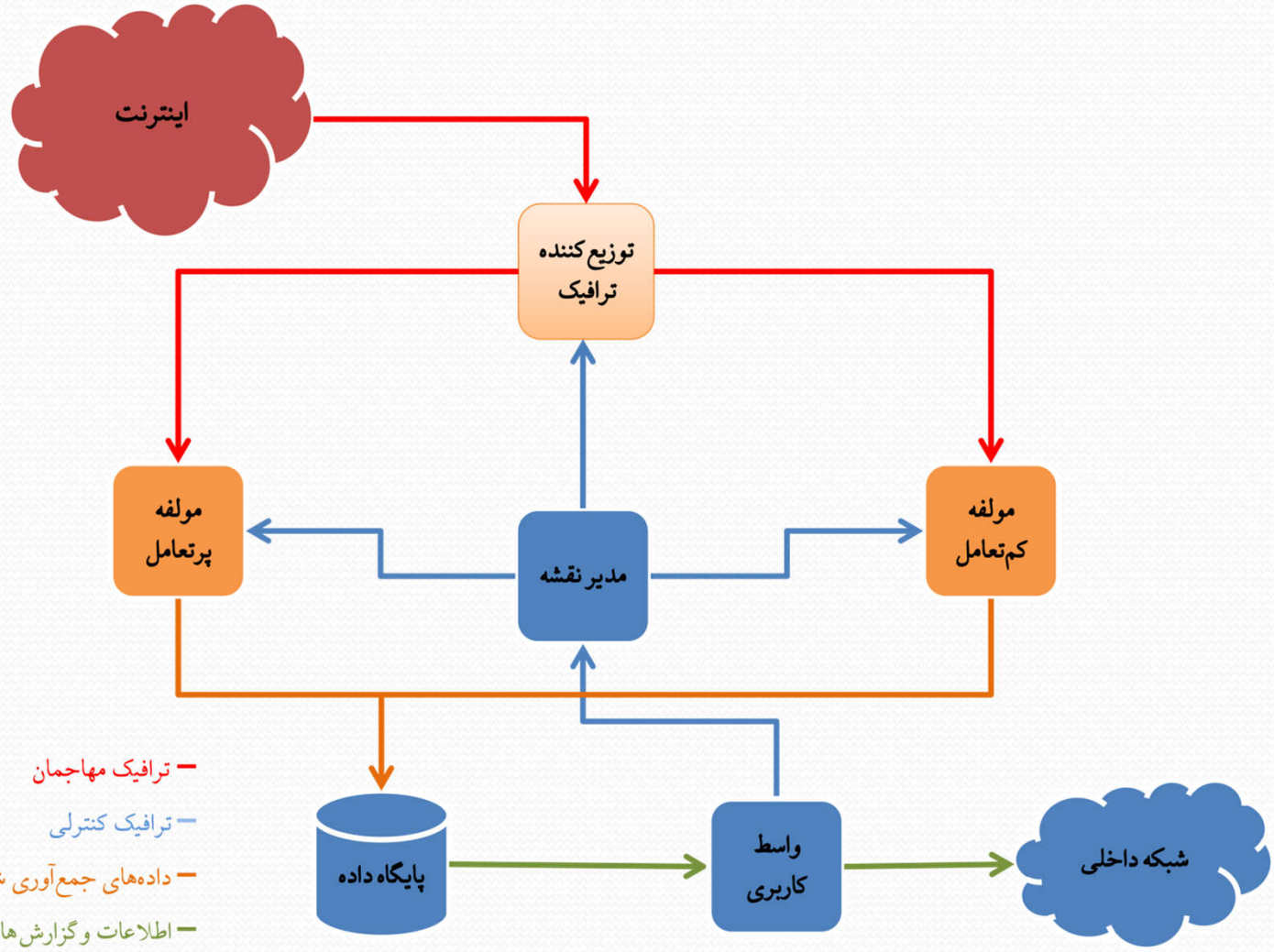
    - کم‌تعامل: شبیه‌سازی محدود خدمات و تعامل حداقلی با مهاجم
    - پرتعامل: ارائه‌ی سرویس آسیب‌پذیر واقعی و تعامل کامل با مهاجم تحت‌نظارت سامانه

فعالیت‌های مرکز آپا شریف – طراحی و توسعه‌ی سامانه

- کم‌تعامل
  - شبیه‌سازی محدود خدمات و تعامل حداقلی با مهاجم
  - هدف کشف بدافزارها، کرمها و ...
- پرتعامل

ارائه‌ی سرویس آسیب‌پذیر واقعی و تعامل کامل با مهاجم تحت‌نظارت سامانه

فعالیت‌های مرکز آپا شریف – طراحی و توسعه‌ی سامانه



فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- طراحی و پیاده‌سازی سیستم کنترل دسترسی چندسطحی در پایگاه‌داده‌ها
  - مطالعات تطبیقی
  - طراحی مدل کنترل دسترسی
  - طراحی مکانیزم
  - پیاده‌سازی در PostgreSQL

فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- بررسی و مطالعه‌ی انواع روش‌های موجود در پایگاه‌داده‌های رمزشده
- تدوین ره‌نگاشت توسعه‌ی سیستم مدیریت پایگاه‌داده‌ی بومی امن

فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- رمزنگاری پنهان داده (TDE) در سیستم مدیریت پایگاه‌داده‌ی بومی

برای امنیت داده‌ها با سه مسئله مواجه هستیم:

- امنیت داده‌های در انتقال،
- امنیت داده‌های ذخیره شده،
- امنیت داده‌های در حال پردازش.

فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- یکی از مکانیزم‌های موجود برای محافظت از داده‌های ذخیره‌شده در رسانه‌ی ذخیره‌سازی سمپاد رمزنگاری پنهان داده است که امروزه توسط اکثر سمپادهای تجاری رایج همچون اوراکل، DB2و SQL Serverپشتیبانی می‌شود.
- در رمزنگاری پنهان داده، همانطور که از نام آن مشخص است عملیات رمزنگاری از دید کاربر کاملا پنهان است و کاربر بدون هیچ محدودیتی پرس‌وجوهای خود را اجرا می‌نماید؛ درحالی که داده‌ها به صورت رمز شده در رسانه ذخیره‌سازی، ذخیره می‌شوند.

فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- در سمپاد ارتقاء یافته PostgreSQL که توسط مرکز آپا دانشگاه صنعتی شریف ایجاد شده است، رمزنگاری پنهان داده با قابلیت‌هایی قابل مقایسه و حتی فراتر از سایر سمپادهای تجاری فراهم شده است.

فعالیت‌های مرکز آپا شریف –امنیت پایگاه داده

- ویژگی‌های سمپاد ارتقاء یافته

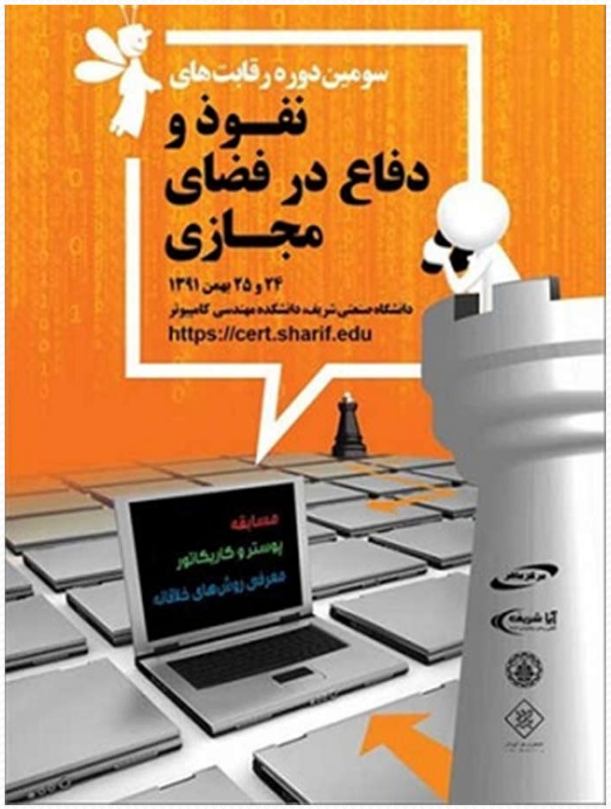
- ✓ رمزنگاری با ریزدانگی ستون و جدول
- ✓ رمز فایل‌های پشتیبان و فایل‌های میانی
- ✓ رمز فایل‌های رویدادنگاری
- ✓ رمز جداول سیستمی
- ✓ تضمین صحت در سطح فایل، ردیف و جداول سیستمی
- ✓ شاخص بر روی داده‌های رمز شده
- ✓ پشتیبانی از کلید خارجی بر روی ستون رمزشده

فعالیت‌های مرکز آپا شریف – رقابت‌های دفاع و نفوذ

مرکز آپا دانشگاه صنعتی شریف از تیرماه ۱۳۹۰ تا کنون رقابت‌های نفوذ و دفاع در فضای مجازی را برگزار نموده است.

فعالیت‌های مرکز آپا شریف – رقابت‌های دفاع و نفوذ

فعالیت‌های مرکز آپا شریف – رقابت‌های دفاع و نفوذ



فعالیت‌های مرکز آپا شریف – رقابت‌های دفاع و نفوذ

رقابت‌های دفاع و نفوذ – اهداف

- فرهنگ سازی و ارتقای آگاهی، دانش و مهارت در زمینه امنیت فضای تبادل اطلاعات و ارتباطات (افتا) است.
- این رقابت‌ها فرصت مناسبی برای تیم‌ها و افراد فعال در این حوزه فراهم می‌سازد تا توانمندی‌ها و قابلیت‌های تخصصی خود را ارزیابی کنند.
- فراهم آوردن زمینه‌ی تبادل دانش و تجربیات بین این افراد، امکان ایجاد تعاملات مناسب را بین افراد درگیر و موثر در این حوزه فراهم سازد.

رقابت‌های دفاع و نفوذ –محورها

- ارائه روش‌های خلاقانه در نفوذ و دفاع
- کارگاه‌های آموزشی و تخصصی
- پوستر و کاریکاتورهای ترویجی
- رقابت فتح پرچم
- کشف شواهد رایانه‌ای

ارائه روش‌های خلاقانه در نفوذ و دفاع

ارائه آخرین دستاوردها و روش‌های خلاقانه و کاربردی نفوذ و دفاع در فضای مجازی و ایجاد بستری برای معرفی توانمندی‌های دانشی فعالان حوزه امنیت، هدف اصلی این محور از مسابقات بوده است.

- معرفی آسیب‌پذیری‌های جدید و روش‌های نفوذ در سرویس‌ها، پروتکل‌ها و برنامه‌ها، روش‌های تحلیل،
- شکست یا کشف ضعف در الگوریتم‌های رمزنگاری و توابع درهم‌ساز،
- روش‌های نوین نفوذ به سیستم در سطح سخت‌افزاری،
- روش‌های نوین در مهندسی معکوس،
- روش‌های امن‌سازی در حوزه‌های نوظهور با رویکردی کاربردی

ارائه روش‌های خلاقانه در نفوذ و دفاع

- طراحی و پیاده‌سازی روت‌کیت‌های اندرویدی مبتنی بر سازوکار تبادل پیام
- فروپاشی از درون: معرفی و شرح حمله «جعل درخواست از سوی سرور»
- ارایه یک روش نوین جهت تشخیص تخطی از روال اجرا
- روشی جهت حمله به ابزار کشف بدافزار با رویکرد جلوگیری از رهگیری فراخوانی‌های سیستمی
- Call-Oriented Programming ShellCodes

کارگاه‌های آموزشی و تخصصی -برخی از کارگاه‌ها

- در بخش کارگاه‌های آموزشی، کارگاه‌های مختلفی در حوزه امنیت فضای تبادل اطلاعات برگزار خواهد شد.

- کارگاه‌های رقابتهای دوره هفتم در هفته اول دی ماه برگزار خواهد شد.

کارگاه‌های آموزشی و تخصصی -برخی از کارگاه‌ها

- کارگاه تخصصی با عنوان Real World Security Audit-Scenario Workshop
- کارگاه تخصصی با عنوان Mobile Signature as a Service
- کارگاه آموزشی تحلیل و مقابله با بدافزار مقدماتی (تحلیل ایستا)

پوستر و کاریکاتورهای ترویجی

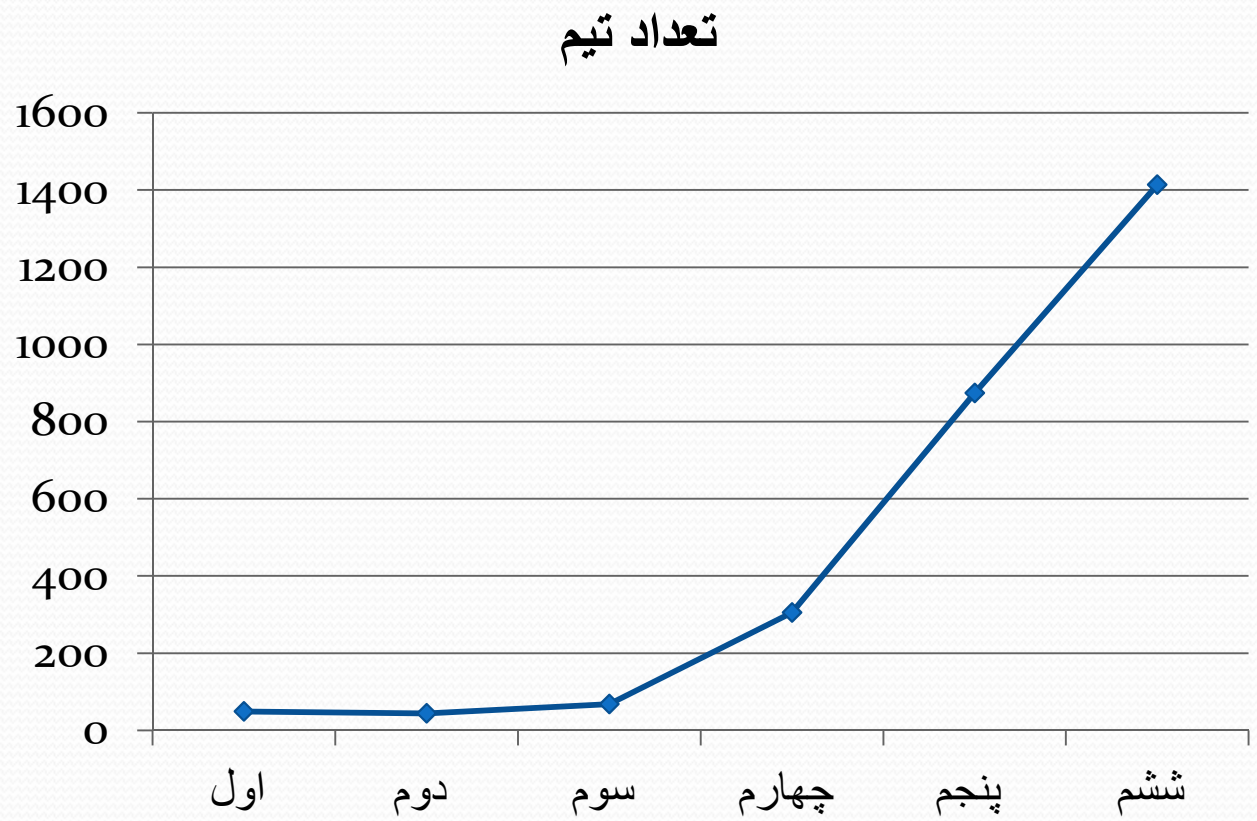
- هدف این بخش، تولید اثرهایی است که با هدف آگاهی‌رسانی امنیتی به مخاطبان عام ایجاد می‌شوند.
- چالش اصلی در این بخش، که انتخاب اثرها نیز بر اساس آن صورت می‌پذیرد، ایجاد یک اثر خلاقانه، جذاب و موثر است که حاوی پیامی ساده درباره‌ی یک یا چند موضوع مهم در حوزه‌ی امنیت اطلاعات در جامعه باشد.
- شرکت‌کنندگان می‌توانند پیامی تصویری و گرافیکی را در خصوص هر یک از مباحث امنیتی مطرح در فضای تبادل اطلاعات ارایه دهند.

رقابت‌های فتح پرچم

Capture The Flag

- رقابت‌های فتح پرچم از رایج ترین رقابت‌های امنیت در دنیاست.
- رقابت‌های سه دوره اخیر مرکز به صورت بین‌المللی برگزار شده است.

رقابت‌های فتح پرچم

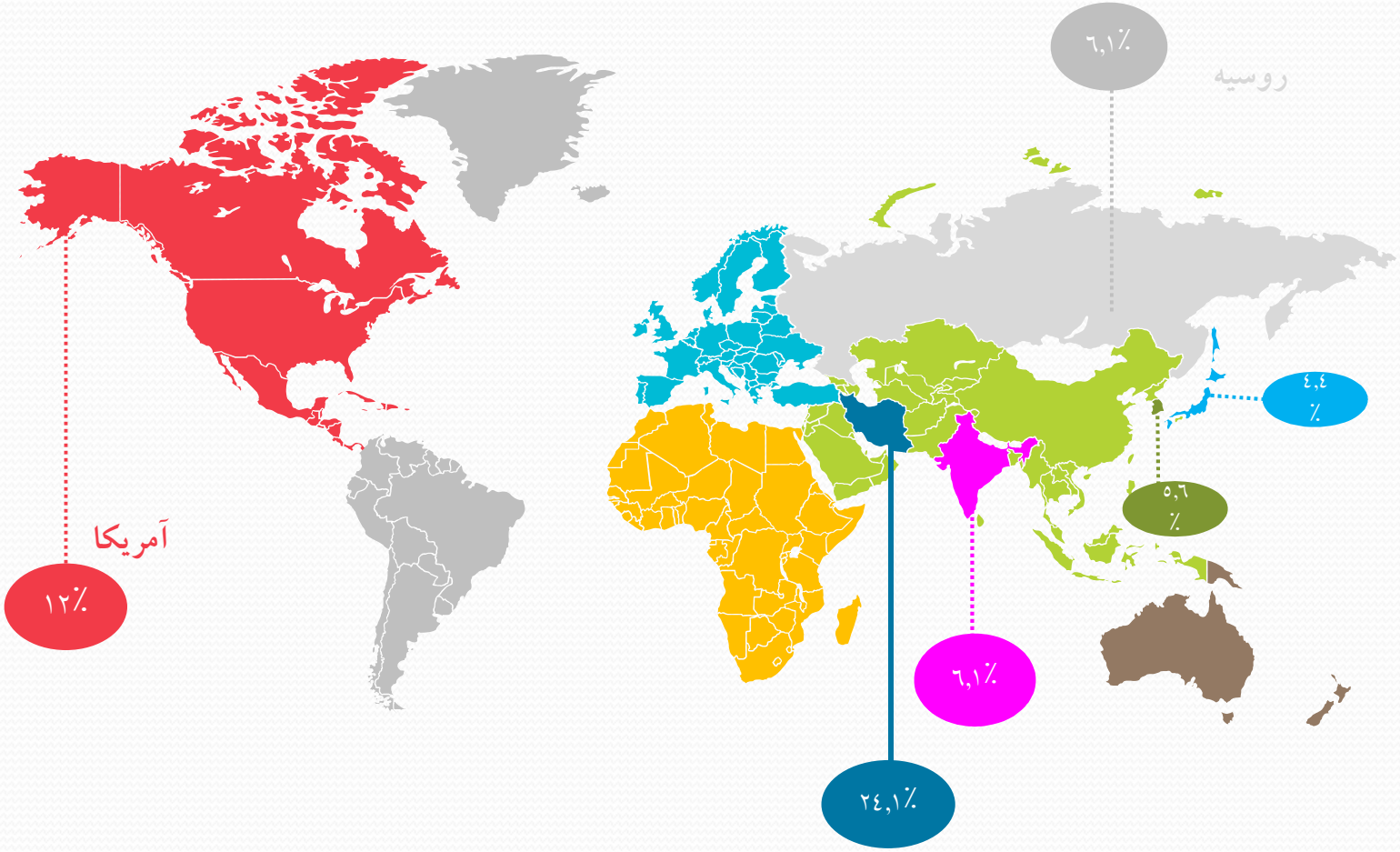


رقابت‌های فتح پرچم – دوره ششم

- تعداد ۳۶ چالش در ۶ زمینه در طی ۳۶ ساعت در اختیار شرکت کنندگان قرار گرفت.
- ۱۴۱۴ تیم ایرانی و خارجی در این دوره از رقابت‌ها به رقابت پرداختند.
- در مقایسه با ۸۳۷ تیم شرکت‌کننده در سال گذشته، تعداد شرکت‌کنندگان به طرز چشمگیری افزایش یافته است.
- ۳۴۹ تیم ایرانی در این رقابت‌ها ثبت‌نام کردند.
- ۴۴۷ تیم در نهایت موفق به کسب امتیاز شدند.
- شرکت کنندگان از ۹۹ کشور ثبت‌نام کردند.

رقابت‌های فتح پرچم – دوره ششم

رقابت‌های فتح پرچم – دوره ششم



رقابت‌های فتح پرچم – ثبت نام

- ثبت نام از طریق

http://ctf.sharif.edu

با تشکر از توجه شما ...

مرکز آپا دانشگاه صنعتی شریف

http://cert.sharif.edu